USER GUIDE

Recover Lost or Forgotten Passwords

Password Recovery Toolkit™

Recover Passwords Quickly & Easily

AccessData

AccessData PRTK 6.5 & DNA 3.5 User Guide

LEGAL INFORMATION

AccessData Corp. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Corp. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, AccessData Corp. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Corp. reserves the right to make changes to any and all parts of AccessData software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

©2010 AccessData Corp. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

AccessData Corp.
384 South 400 West
Suite 200
Lindon, Utah 84042
U.S.A.

www.accessdata.com

ACCESSDATA TRADEMARKS

- AccessData® is a registered trademark of AccessData Corp.
- Distributed Network Attack® is a registered trademark of AccessData Corp.
- DNA® is a registered trademark of AccessData Corp.
- Forensic Toolkit® is a registered trademark of AccessData Corp.
- FTK® is a registered trademark of AccessData Corp.
- Password Recovery Toolkit® is a registered trademark of AccessData Corp.
- PRTK® is a registered trademark of AccessData Corp.
- Registry Viewer® is a registered trademark of AccessData Corp.

DOCUMENTATION CONVENTIONS

In AccessData documentation, a number of text variations are used to indicate meanings or actions. For example, a greater-than symbol (>) is used to separate actions within a step. Where an entry must be typed in using the keyboard, the variable data is set apart using [*variable_data*] format. Steps that required the user to click on a button or icon are indicated by *italics*.

A trademark symbol (®, ™, etc.) denotes an AccessData trademark. Unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

REGISTRATION

The AccessData product registration is done at AccessData after a purchase is made, and before the product is shipped. The licenses are bound to either a USB security device, or a Virtual CmStick, according to your purchased.

SUBSCRIPTIONS

AccessData provides a one-year licensing subscription with all new product purchases. The subscription allows you to download and install the latest releases for your licensed products during the active license period. Following the initial licensing period, a

subscription renewal is required annually for updating your products. You can renew your subscriptions through your AccessData Sales Representative.

Use LicenseManager to view your current registration information, to check for product updates and to download the latest product versions, where they are available for download. You can also visit our web site, www.accessdata.com anytime to find the latest releases of our products.

For more information, see ManagingLicenses in your product manual or on the AccessData web site.

ACCESSDATA CONTACT INFORMATION

Your AccessData Sales Representative is your main contact with AccessData Corp. Also, listed below are the general AccessData telephone number and mailing address, and telephone numbers for contacting individual departments.

MAILING ADDRESS AND GENERAL PHONE NUMBERS

You can contact AccessData in the following ways:

TABLE Front-1 AD Mailing Address, Hours, and Department Phone Numbers

Corporate Headquarters:	AccessData Corp. 384 South 400 West Suite 200 Lindon, UT 84042 USA **Voice**: 801.377.5410 **Fax**: 801.377.5426
General Corporate Hours:	Monday through Friday, 8:00 AM – 5:00 PM (MST) AccessData is closed on US Federal Holidays
State and Local Law Enforcement Sales:	**Voice**: 800.574.5199, option 1 **Fax**: 801.765.4370 **Email**: Sales@AccessData.com
Federal Sales:	**Voice**: 800.574.5199, option 2 **Fax**: 801.765.4370 **Email**: Sales@AccessData.com
Corporate Sales:	**Voice**: 801.377.5410, option 3 **Fax**: 801.765.4370 **Email**: Sales@AccessData.com
Accounting:	**Voice**: 801.377.5410, option 4

TABLE Front-1 AD Mailing Address, Hours, and Department Phone Numbers

Training:	**Voice**: 801.377.5410, option 6 **Fax**: 801.765.4370 **Email**: Training@AccessData.com

TECHNICAL SUPPORT

You can contact AccessData Customer and Technical Support in the following ways:

TABLE Front-2 AD Customer & Technical Support Contact Information

Customer Service Hours:	Monday through Friday, 7:00 AM – 6:00 PM (MST)
Customer/Technical Support: Free technical support is available on all AccessData products.	**Voice**: 801.377.5410, option 5 **Voice**: 800.658.5199 (Toll-free North America) **Email**: Support@AccessData.com **Web site**: http://www.AccessData.com/Support

The Support web site allows access to Discussion Forums, Downloads, Previous Releases, our Knowledgebase, a way to submit and track your "trouble tickets", and in-depth contact information.

Note: All support inquiries are typically answered within one business day. If there is an urgent need for support, contact AccessData by phone during normal business hours.

DOCUMENTATION

Please email us regarding any typos, inaccuracies, or other problems you find with the documentation to:
documentation@accessdata.com

PROFESSIONAL SERVICES

The AccessData Professional Services staff comes with a varied and extensive background in digital investigations including law enforcement, counter-intelligence, and corporate security. Their collective experience in working with both government and commercial entities, as well as in providing expert testimony, enables them to provide a full range of computer forensic and eDiscovery services.

At this time, Professional Services provides support for sales, installation, training, and utilization of FTK, Enterprise, eDiscovery, Lab, and Lab Lite. They can help you resolve any questions or problems you may have regarding these products.

CONTACT INFORMATION FOR PROFESSIONAL SERVICES

- Washington DC: 410.703.9237
- North America: 800.574.5199
- International: +1.801.377.5410
- **Email**: adservices@accessdata.com

Table of Contents

AccessData PRTK 6.5 & DNA 3.5 User Guide ..... *i*
Legal Information ..... *i*
AccessData Trademarks ..... *ii*
Documentation Conventions ..... *ii*
Registration ..... *ii*
Subscriptions ..... *ii*
AccessData Contact Information ..... *iii*
Mailing Address and General Phone Numbers ..... *iii*
Technical Support ..... *iv*
Documentation ..... *iv*
Professional Services ..... *iv*
Contact Information for Professional Services ..... *v*

Table of Contents ..... *vii*

Chapter 1 Overview *1*
PRTK and DNA Overview *1*
Features Overview *2*
Other AccessData Decryption Products *3*
PRTK / DNA Add-Ons *3*
License Management Products *5*
Audience *5*

Chapter 2 Installing PRTK 6.5 & DNA 3.5 7
Before Installing PRTK or DNA 7
Planning the Installation 7
PRTK or DNA Installation Prerequisites 8
Installing PRTK 9
Installing LicenseManager 12
Installing DNA 12
Supervisor Installation 13
DNA Worker Installation 16
After Installing PRTK or DNA 26
Uninstalling PRTK or DNA 26
Uninstalling PRTK 26
Uninstalling the DNA Supervisor 27
Uninstalling the DNA Worker 28
To Uninstall a Linux, Mac, or PS3 Worker 29

Chapter 3 Getting Started 31
Starting PRTK or DNA 31
Using the USB Security Device 32
Running PRTK or DNA in Demo Mode 32
Right-click Menus 33
Viewing Module Information 33
Customizing the User Interface 33
Showing or Hiding Elements 33
The Menu Bar 35
Changing Preferences 39
The Toolbar 44
The Job Queue Pane 45
Changing Attributes Order in the Job Queue Pane 47
Sizing Column Headings in the Job Queue Pane 47
The Properties Pane 48
DNA User Interface 49

Priority Groups Pane *49*

Chapter 4 Managing DNA 3.5 System Configurations *51*

Disconnecting From and Connecting to the DNA Service *52*
Stopping and Restarting the Supervisor Service *52*
Restarting the Worker *53*
Backing Up and Restoring Keys *54*
Backing Up Keys *54*
Restoring Keys *55*
Viewing Workers Information From the Supervisor Machine *55*
Viewing Worker Information From the Worker Machine *56*
Understanding the DNA Worker Interface *57*
Managing Workers and Groups *58*
Filtering the Workers List *58*
Monitoring a DNA Worker *60*
Creating a Group *65*
Editing a Group *66*
Deleting a Group *68*
Changing the Group Membership of a DNA Worker *68*
Changing the Supervisor of a DNA Worker *70*

Chapter 5 Recovering Passwords *71*

Recovery Process Overview *71*
Best Practices for Adding Jobs *73*
Adding Jobs *74*
Selecting Files *74*
Dragging and Dropping Files *75*
Monitoring Jobs *75*
Managing the Recovery Process *76*
Specifying Recovery Preferences *77*
Displaying Job Properties *77*
Printing Recovery Reports *86*

Managing Jobs in DNA 87
Allocating Resources for a Job 87
Opening Files Using Recovered Passwords and Keys 90
Manually Decrypting Files with a Password or Key 90

Chapter 6 Managing Profiles 95
Default Profiles 95
Setting a Default Profile 96
Creating a Profile 97
Editing a Profile 99
Deleting a Profile 100

Chapter 7 Managing Password Recovery Rules 101
Understanding Rule Categories 101
Default Rule Order 102
Modifying the Password Rule Order 102
Understanding a User-defined Rule 105
Creating a User-defined Rule 111
Editing a User-defined Rule 113
Removing a User-defined Rule 113

Chapter 8 Using the Dictionary Utility 115
Dictionary Basics 115
PRTK & DNA Dictionary Utility 116
Starting the Dictionary Utility 116
Browse Dictionaries 117
Dictionary Information 118
Standard Dictionary Generator 118
Biographical Dictionary 120
Merge Golden Dictionaries 128

Chapter 9 Specialized Password Recoveries *129*
Recovering Login Passwords *129*
Accessing the SAM File and the System file *129*
Recovering Login Passwords from Windows NT *130*
Recovering Passwords from Win 9x Files *132*
Recovering Login Passwords on Windows 2000 and XP Systems *133*
Recovering Passwords Using a Boot Disk to Access the Files *133*
Processing the Protected System Files in PRTK or DNA *134*
Recovering Passwords from the Windows Registry *135*
Recovering Passwords from the Current Registry *136*
Recovering AOL Communicator Account Passwords *137*
Recovering AOL Instant Messenger Passwords *138*
Recovering AOL Sign-on Passwords *138*
Recovering MSN Messenger Login Passwords *138*
Recovering Netscape .W and .S Files *140*
Recovering QuickBooks Passwords *140*
Recovering Yahoo! Messenger Login Passwords *140*
Recovering WinZip Archive Files *141*
Recovering IE7 ProtectedRegistry (Intelliforms) Files *141*
Collecting Necessary IE7 Files *142*
Steps to Complete *143*
Component Details *144*

Chapter 10 Managing Security Devices and Licenses *147*
NLS Support *147*
Virtual CmStick *147*
Installing and Managing Security Devices *147*
Installing the Security Device *148*
Installing LicenseManager *156*
Managing Licenses with LicenseManager *158*
Starting LicenseManager *160*
The LicenseManager Interface *162*

Opening and Saving Dongle Packet Files *166*
Adding and Removing Product Licenses *167*
Adding and Removing Product Licenses Remotely *168*
Updating Products *171*

Chapter 11 Troubleshooting *173*
PRTK and DNA Troubleshooting *173*
Installation *174*
Password Recovery *175*
DNA Troubleshooting *176*
Add Job Processing Results *178*

Appendix A Recognized Applications and File Formats *179*
Decryption Attack *179*
Dictionary Attack *182*
Keyspace Attacks *186*
Reset Attacks *187*
Multiple Attacks *187*

Appendix B Password Recovery Attacks *193*
Languages *193*
Character Groups *193*
Default Dictionaries *194*
Rules *196*
Default Rule Order *197*
Profiles *202*
English *202*
Arabic *204*
European *207*
Russian *209*
Pass-phrase *211*

FTK Import 212
PRTK 212
DNA 214
Character Replacements 215
Common Prefixes 215
Common Suffixes (a.k.a. Postfixes) 216
Prepositional and Verb Phrases 216

Appendix C Encryption Technology 217
Understanding Encrypted Files 217
Understanding the PRTK & DNA Decryption Process 218
Decryption Attack 219
Dictionary Attack 219
Keyspace Attack 220
Reset Attack 220
Current Encryption Standards 220
Symmetric Encryption 220
RC4 221
Asymmetric Encryption 221
Hashing 222
Secure Hash Algorithm (SHA) 222
Message Digest 5 (MD5) 222

Appendix D Program Files 223
PRTK Files 223
DNA Supervisor Files 225

Appendix E Recovering EFS Files 229
Recovering EFS on Windows XP Service Pack 1 or Later 229
Other Notes 230

AccessData Glossary 231

Chapter 1 Overview

This AccessData® product manual covers both Password Recovery Toolkit®(PRTK®) 6.5 and Distributed Network Attack® (DNA®) 3.5. Both are used in many different environments to provide specific, password-cracking related functions. For example, law enforcement and corporate security professionals can use PRTK and DNA in computer forensic investigations to access password-protected files. IT administrators can use PRTK and DNA to recover system passwords, while individual users can use PRTK and DNA to recover lost passwords to personal files. These two products provide access to passwords for many popular applications in the industry.

PRTK runs on a single machine only. DNA uses multiple machines across the network or across the world to conduct key space and dictionary attacks. In many cases, this makes use of time those computers would normally be idle, saving the cost of additional hardware. Many times, the cost of additional hardware is justified for a secure, dedicated password recovery lab.

These and other differences are covered in this manual. In general when referring to PRTK features, you can assume that the same applies to DNA. The PRTK user interface is slightly different from that of DNA, so for those differences, you will need to refer to the DNA-specific sections of this manual for information regarding DNA-only features.

For more information about PRTK, DNA, or any other AccessData product, see the AccessData website at www.accessdata.com.

PRTK AND DNA OVERVIEW

With this release, PRTK and DNA have essentially the same program interface and they work essentially the same way. Both programs analyzes file signatures to find encryption types and determine which recovery modules to use. See "Understanding Encrypted Files" on page 217.

Before recovering passwords for protected files, PRTK and DNA create hash values that can be used to aid in determining whether the content of a file changed during the password recovery.

PRTK and DNA perform recoveries on protected files using various methods, including decryption and dictionary attacks. For more information on attack types, see "Understanding the PRTK & DNA Decryption Process" on page 218. For difficult password key values, PRTK performs dictionary attacks using various types of dictionaries, including the Golden Dictionary (containing previously recovered passwords), as well as Biographical, Custom User, and Default dictionaries.

PRTK and DNA display basic file, or job, information for jobs in the Properties Pane, and more extensive information in the Job Properties window.

After recovering passwords, you can print reports, and open recovered files.

FEATURES OVERVIEW

PRTK and DNA perform the following basic functions:

- Hash files

  Hashing a file uses an algorithm that creates a unique hash value for a file, allowing verification that the contents of a file remain unchanged. When a file is added to PRTK or DNA for key or password recovery, it is hashed. When the key or password is recovered, the file is automatically hashed again to verify that the file itself has remained unchanged. This is particularly helpful to law enforcement personnel who need to verify that a file has not been changed while recovering a password.

- Recover passwords

  PRTK can recover the password to files created in many popular industry applications by using a variety of methods, including several types of dictionaries used within profiles, in combination with rules to achieve the desired results. PRTK can also recover multi-lingual passwords.

- Generate reports

  You can now print job information reports for password recovery jobs in .PDF format.

- Open encrypted files

You can use recovered keys or passwords to open recovered files, if the applications the files originated from are available and installed on a computer you have access to. Recovered files can be copied or moved to any location.

Other AccessData Decryption Products

AccessData has developed other industry-leading products to assist in password recovery. The following sections offer a brief introduction to these products. For more information on any of these or any AccessData products, please visit our website, www.accessdata.com.

PRTK / DNA Add-Ons

The following add-ons are available to enhance the power and speed of password-cracking with PRTK and/or DNA:

Rainbow (Hash) Tables

Rainbow Tables are pre-computed, brute-force attacks. In cryptography, a brute-force attack is an attempt to recover a cryptographic key or password by trying every possible key combination until the correct one is found. How quickly this can be done depends on the size of the key, and the computing resources applied.

A system set at 40-bit encryption has one trillion keys available. A brute-force attack of 500,000 keys per second would take approximately 25 days to exhaust the key space combinations using a single 3 GHz Pentium 4 computer. With a Rainbow Table, because all possible keys in the 40-bit keyspace are already calculated, file keys are found in a matter of seconds-to-minutes; far faster than by other means. DNA and PRTK seamlessly integrate with Rainbow Tables.

Product Features

Three Rainbow Tables Hash Sets are available:

- MS Office Word and Excel
- Acrobat PDF
- Windows LAN Hash

Each hash set takes nearly 3TB of disk space.

AccessData RainbowTables hash sets for Windows LAN Hash ship with their own user-interface program, and that is the one that should be used for LAN Hash files. The Rainbow Tables has sets for MS Office and Acrobat PDF, as well as the Portable Office Rainbow Tables, (PORT) all run with AccessData Rainbow Tables stand-alone user-interface program. Check for the latest version of RainbowTables.exe on the AccessData Website, www.AccessData.com.

PORTABLE OFFICE RAINBOW TABLES

Rainbow Tables are also pre-computed, brute-force attacks. AccessData Portable Office Rainbow Tables (PORT) are different from the full Hash tables set. A statistical analysis is done on the file itself to determine the available keys. This takes far less space than the Hash Tables, but also takes somewhat more time and costs a small percentage in accuracy.

As previously stated, a system set at 40-bit encryption has one trillion keys available. A brute-force attack of 500,000 keys per second would take approximately 25 days to exhaust the key space combinations of a single file using a single 3 Ghz Pentium 4 computer. With Portable Office Rainbow Tables, you can decrypt 40-bit encrypted files Microsoft Word or Excel files, usually in seconds, minutes, or hours, rather than days or weeks, depending on the power of the system you are using. PORT is a standalone product and does not require DNA or PRTK to be installed on the computer where it is run. It does, however, require a valid license.

Product Features

- 40-bit encrypted files decrypted in 5 minutes on average
- One table available: MS Word & Excel (MS Office)
- 98.6% accuracy for MS Office Word and Excel files.
- Completely portable, fits on your laptop

PORT for Word and Excel takes only about 3.7 GB of disc space. It is shipped on a single DVD. You can carry it with you! Indispensable for on-site acquisitions and investigations.

TACC UNIT

The Tableau TACC1441 Hardware Accelerator (TACC) is a specialized product that reduces the dictionary-based password recovery times of PRTK and DNA. The TACC accelerator performs massively parallel, high-speed computations of cipher-keys, yielding a dramatic increase in the number of passwords per second that each host computer generates. This results in a greater number of successful attacks in a

significantly shorter amount of time. For more information, contact your AccessData sales rep, or contact Tableau, LLC; www.tableau.com.

License Management Products

LicenseManager

AccessData LicenseManager lets you manage product and license subscriptions stored on your Wibu CodeMeter USB or Virtual CmStick or Keylok dongle USB license security device. LicenseManager communicates directly with AccessData's license server, so when license renewals take place, the information is readily and immediately accessible for download to your license device.

LicenseManager checks for the newest releases of your installed products, and also tells you when your license is near expiration.

CodeMeter Runtime

The CodeMeter Runtime Kit is a program that is designed to work with the Wibu CodeMeter USB or Virtual CmStick so AccessData programs can verify license information stored on the CmStick. It must be installed prior to connecting the CmStick. The CmStick and CodeMeter Runtime Kit software must be fully installed prior to running LicenseManager. Either a CmStick, or a Keylok dongle with a current license is required to fully utilize PRTK or DNA. CodeMeter Runtime can be installed and running on the same machine with the AccessData Dongle Drivers, but both hardware devices cannot be connected to the same machine at the same time.

For more information regarding the WIBU-SYSTEMS products utilized by AccessData, see "Chapter 10 Managing Security Devices and Licenses" on page 147.

Audience

PRTK and DNA are intended for law enforcement officials and corporate security and IT professionals who need access to password-protected files, folders, and computers. PRTK is also available for any individual, such as an administrator or user, who needs to recover a lost or forgotten password. PRTK and DNA can also be used as a security risk assessment tool to identify the weakest links in an organization's security profile.

Anyone using PRTK should possess the following competencies:

- Basic knowledge of and experience with personal computers

- Understanding of file protection through passwords and cryptographic standards
- Familiarity with the Microsoft Windows environment

In addition, law enforcement and corporate security professionals should possess the following competencies:

- Basic knowledge of and training in forensic policies and procedures
- Familiarity with the fundamentals of collecting digital evidence and ensuring the legal validity of the evidence
- Understanding of forensic images and how to acquire forensically sound images
- Experience with case studies and reports

Chapter 2 Installing PRTK 6.5 & DNA 3.5

This chapter describes how to install and uninstall AccessData® Password Recovery Toolkit® (PRTK®) and AccessData Distributed Network Attack® (DNA®).

BEFORE INSTALLING PRTK OR DNA

Before installing PRTK or DNA, you should evaluate the workstation and its current software according to your investigational needs. A good understanding of the workstation and its configured devices can help ensure that PRTK or DNA runs efficiently, and does not degrade the performance of your other applications.

PLANNING THE INSTALLATION

Before installing either PRTK or DNA, you must consider the following:

- Role of the workstation

  Determine if it is used as a regular user workstation, a forensic analysis workstation, or a password recovery machine.

- Access policy

  To prevent security issues, identify where the system is located, when the cases can be worked on, and ensure that only the desired personnel can access the system and its information.

- Hardware and software requirements

  For the hardware and software requirements, see the AccessData Web site, www.accessdata.com. In addition, the System Requirements.PDF can be found on

the installation disc, beginning with this release, and is also available in the DNA 3 or PRTK 6 folder structure after installation.

- Application relationships

  Verify that your installed applications can work simultaneously. Also, do not run so many applications that you compromise overall performance.

- You cannot install both PRTK and the DNA Supervisor on the same machine. You must install one or the other.

- Network and Internet issues

  Determine whether the workstation should be connected to a network or the Internet. Under normal circumstances, the forensic analysis workstation is not constantly connected to the Internet to avoid the possibility of tainting evidence. While there are some reasons to be connected to the Internet, most tasks requiring Internet access can be accomplished through other means.

- System policies and procedures

  Check with your system administrator about any specific security policies and procedures that might exist that may change the installation plan.

- Administrator rights

  To run PRTK or DNA successfully, you must be logged in as an administrator with full admin rights on the local machine where PRTK or DNA is installed.

PRTK OR DNA INSTALLATION PREREQUISITES

Before running the PRTK or DNA installation, you must install either the WIBU-SYSTEMS CodeMeter Runtime Software and CodeMeter license security device (also known as a CmStick), or the CodeMeter software, AccessData dongle driver, and Keylok USB dongle license security device.

For more information about installing and using license security devices, related software, and LicenseManager, see "Chapter 10 Managing Security Devices and Licenses" on page 147.

You will need:

- The WIBU-SYSTEMS 32- or 64-bit CodeMeter Runtime software with a WIBU-SYSTEMS CodeMeter (CmStick)

  OR

- The WIBU-SYSTEMS 32- or 64-bitCodeMeter Runtime software, and the AccessData 32- or 64-bit Dongle Drivers with a Keylok dongle

- If you will be using Rainbow Tables or PORT, you must have the WIBU-SYSTEMS 32- or 64-bitCodeMeter Runtime software, and the AccessData 32- or 64-bit Dongle Drivers with a Keylok dongle
- The Codemeter Runtime software and either a silver WIBU-SYSTEMS CmStick or a green Keylok dongle and its related drivers are required to run PRTK or DNA. Without them, you can run PRTK or DNA in Demo mode only. Registry Viewer is the only other program that has a demo mode available.

The CmStick or dongle should be stored in a secure location when not in use.

You can install PRTK or DNA from its shipping CD or from downloadable files available on the AccessData web site at www.accessdata.com. Click *Support* > *Downloads*, and browse to the product to download. Click the download link and save the file locally prior to running the installation files.

Once you have installed the dongle drivers, connected the license security device, and verified that Windows recognizes it, you can use LicenseManager to manage product licenses.

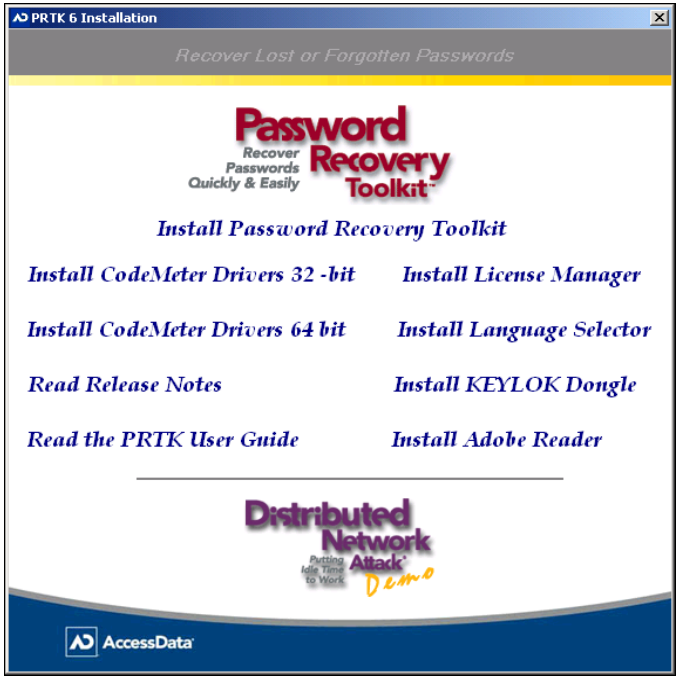
INSTALLING PRTK

To install PRTK from the CD, do the following:

1. Insert the CD into the CD-ROM drive and wait for the PRTK 6 Installation screen to display.

   If auto-run is not enabled, select *Start* > *Run*. Browse to the CD-ROM drive and select Autorun.exe.

2. Click *Install Password Recovery Toolkit*.



3. Click *Next* on the Welcome screen.

AccessData Password Recovery Toolkit - InstallShield Wizard
AccessData
Password Recovery Toolkit
The InstallShield Wizard will install AccessData Password Recovery Toolkit on your computer. To continue, click Next.
< Back
Next >
Cancel

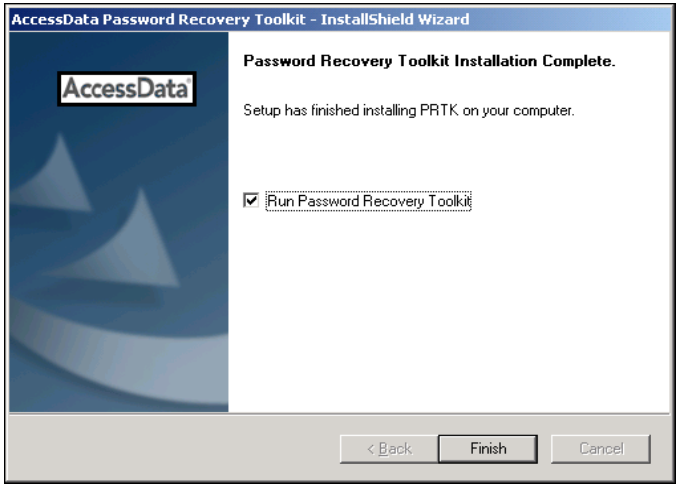
4. Read and accept the License Agreement, then click *Next*.

AccessData Password Recovery Toolkit - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
AccessData
AccessData® Corp. End User License Agreement
THIS IS A LEGAL AGREEMENT between "you," the end user of AccessData Corp. brand software, and AccessData Corp. (AccessData).
Use of the software you have downloaded or are about to install indicates your acceptance of these terms. As used in this Agreement, the capitalized term "Software" means the AccessData® software together with any and all enhancements, upgrades, and updates that may be provided to you in the future by AccessData. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, YOU SHOULD SO INDICATE AT THE APPROPRIATE SCREEN AND PROMPTLY DISCONTINUE THE INSTALLATION AND DOWNLOAD PROCESS.
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
InstallShield
< Back
Next >
Cancel

- If you choose not to accept the terms of the license agreement, you cannot continue with the installation.
- You can print the License Agreement by clicking *Print*. You must have a printer already installed to do so.

The product installation begins. A progress bar shows the status of the installation.

5. When the installation is complete, you will see the following screen.



6. Mark *Run Password Recovery Toolkit* if you want to run the program now.

OR

Unmark *Run Password Recovery Toolkit* if you want to run the program later. Make your decision based in part on the following information:

- If you have installed the dongle and the dongle drivers, check *Run Password Recovery Toolkit* to run PRTK after completing the installation.
- If you have not installed the security device and drivers, uncheck *Run Password Recovery Toolkit*, then install the security device and drivers before attempting to run PRTK. Until you complete the process of installing the license security device, you will be able to run the product only in demo mode. For more information on this process, see "Installing and Managing Security Devices" on page 147.

  If you have to install the license security device drivers before you run PRTK, you can start PRTK later by selecting *Start* > *Programs* > *AccessData* > *PRTK 6* > *PRTK*, or by clicking on the PRTK desktop icon.

7. Click *Finish*, return to the home page of the Autorun.exe, and then click

   Install CodeMeter Drivers 32-bit

   OR

   Install CodeMeter Drivers 64-bit, depending on your machine type.
8. If you are running a green Keylok dongle, click *Install KEYLOK Drivers.*
9. Close the Installer.

INSTALLING LICENSEMANAGER

LicenseManager lets you manage product and license subscriptions using a security device or device packet file. For installation instructions and more information, see "Chapter 10 Managing Security Devices and Licenses" on page 147.

Note: You can install LicenseManager from the PRTK or DNA installation disc, or from downloadable files available on the AccessData web site, www.accessdata.com.

INSTALLING DNA

You can install DNA from a CD or from downloadable files available on the AccessData web site, www.accessdata.com.

You need to install CodeMeter Runtime, plus a dongle driver if using a green Keylok dongle instead of the newer WIBU-SYSTEMS USB or Virtual CmStick, the DNA Supervisor, and the DNA Worker(s).

- **Dongle Driver and/or CodeMeter Runtime:** The Keylok dongle or the CmStick enables you to use all features and recovery modules of DNA; the security device software must be installed on the supervisor machine. The CmStick requires only the CodeMeter Runtime software. The Keylok dongle requires The CodeMeter Runtime software and the appropriate Dongle Driver software. Both are available on the AccessData web site.
- **DNA Supervisor:** A machine in the DNA system that controls worker machines in the DNA system, and the jobs that they process. You must install the DNA Supervisor before you install the DNA Workers.
- **DNA Worker:** You must run the appropriate DNA Worker installation program on each participating machine in the system.

The installation copies the files to the [*drive*]:\Program Files\AccessData\DNA 3\ directory, creates the Supervisor folder there, and places files necessary for installing workers, as well as other files there.

Additional files are placed in

[*drive*]:\Documents and Settings\All Users\Application Data\AccessData\PR

This is where you will find Dictionaries, Rules, Profiles, and so forth.

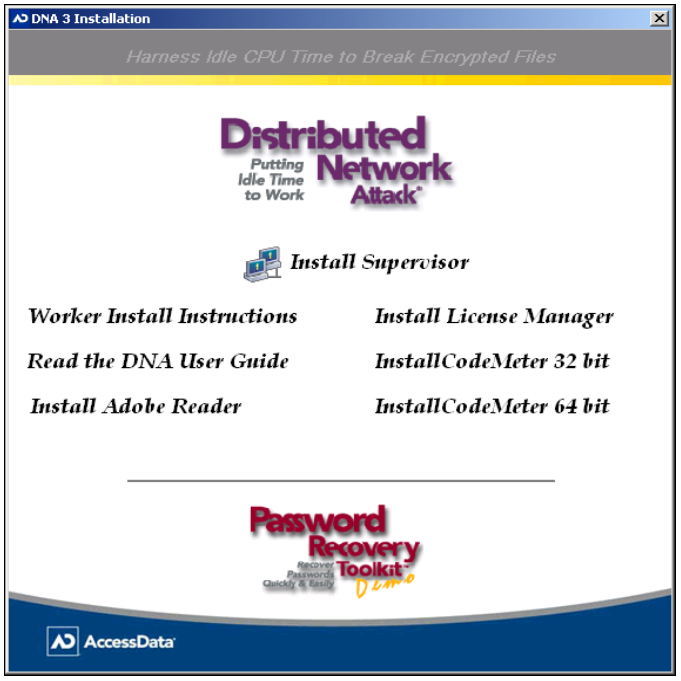
SUPERVISOR INSTALLATION

Run the supervisor installation on the machine that you want to be a DNA Supervisor. Complete the supervisor installation before installing the DNA Worker on any machine.

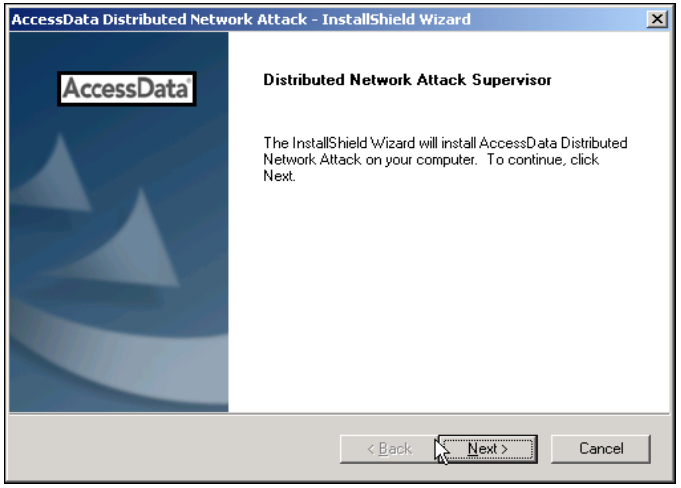
1. Turn off all firewalls, virus scanners, and spyware.
2. Insert the CD into the CD-ROM drive.

   If auto-run is not enabled, select *Start* > *Run*. Browse to the CD-ROM drive. In the Setup folder, double-click Autorun.exe.

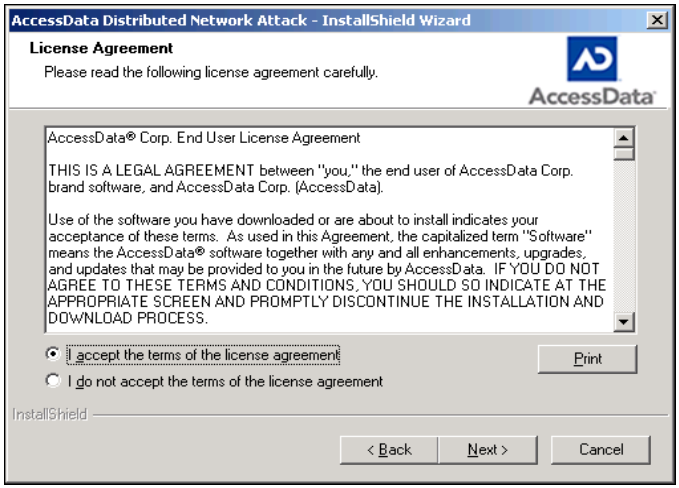
If you are installing from downloadable files, double-click installer file that was downloaded from the AccessData web site.



3. Click *Next* on the Welcome Screen.

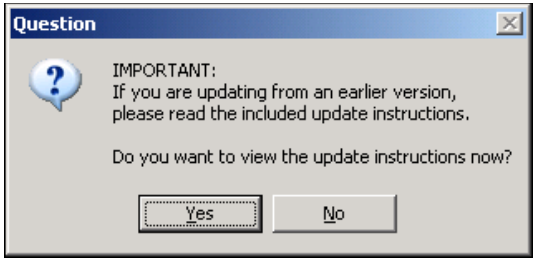

AccessData Distributed Network Attack - InstallShield Wizard
AccessData
Distributed Network Attack Supervisor
The InstallShield Wizard will install AccessData Distributed Network Attack on your computer. To continue, click Next.
< Back
Next >
Cancel

4. Select *I Accept the Terms of the License Agreement.*


AccessData Distributed Network Attack - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
AccessData
AccessData® Corp. End User License Agreement
THIS IS A LEGAL AGREEMENT between "you," the end user of AccessData Corp. brand software, and AccessData Corp. (AccessData).
Use of the software you have downloaded or are about to install indicates your acceptance of these terms. As used in this Agreement, the capitalized term "Software" means the AccessData® software together with any and all enhancements, upgrades, and updates that may be provided to you in the future by AccessData. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, YOU SHOULD SO INDICATE AT THE APPROPRIATE SCREEN AND PROMPTLY DISCONTINUE THE INSTALLATION AND DOWNLOAD PROCESS.
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
InstallShield
< Back
Next >
Cancel

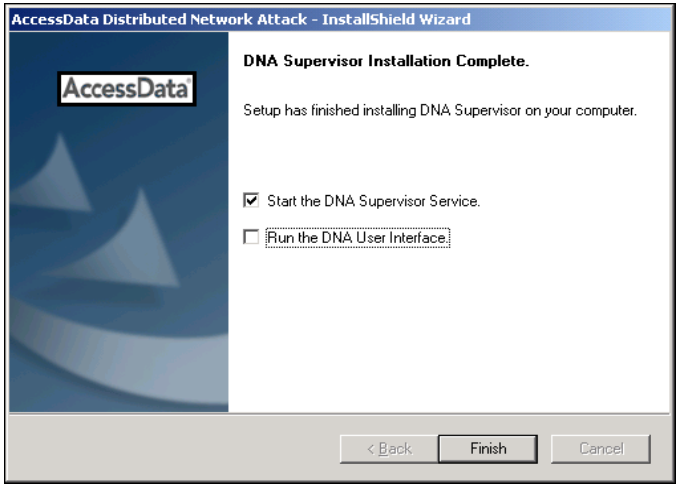
If you choose not to accept the terms of the license agreement, you cannot continue with the installation.

5. Click *Print* to print the license agreement. You must have already installed a printer.
6. (Conditional) If you have already completed a partial uninstall and want to re-install the supervisor using your saved keys, when prompted, click *Yes*; then browse to and select the Supervisor.ini file.


Question
IMPORTANT:
If you are updating from an earlier version, please read the included update instructions.
Do you want to view the update instructions now?
Yes
No

7. If you are updating from an earlier version, click *Yes* to view the update instructions, or *No* to continue without viewing the update instructions.

7a. If you are updating from an earlier version, choose to view the Readme when prompted.



8. Check *Start the DNA Supervisor Service*. Do not mark *Run the DNA User Interface* at this time. You will need to install the worker(s) before running the DNA User Interface.
9. Click *Finish* to complete the installation on the Supervisor Installation Complete form.
10. Follow the steps to install workers for your DNA system as described below.

DNA Worker Installation

Before you begin this installation, the Supervisor folder on the Supervisor machine should be shared to allow worker machines to remotely access it for running the DNA Worker installation.

Important: You **must not** compress the Worker.ini file.

The DNA Worker installation programs are available in the Supervisor directory. You can install the DNA Worker on Windows, Macintosh, Linux, or PS3 machines. For more information about the worker system requirements, see the System Requirements.pdf file in the Supervisor folder.

Sharing the Supervisor Directory

Share the Supervisor directory to allow worker machines to remotely access it for running the DNA Worker installation.

If the directory isn't already shared, complete the following:

In Windows Explorer, navigate to the [*drive*]: Program Files\AccessData\DNA 3\ directory. Right-click the \Supervisor\ directory and select *Sharing*.

1. In the Sharing tab, select *Shared As*.
2. (Optional) Enter any additional information in the Sharing tab fields that you want to require of the client workstations before they can access the directory.

DNA WORKER INSTALLATION ON A WINDOWS WORKSTATION

Before you begin this installation, the Supervisor folder on the Supervisor machine should be shared to enable the workers to access the worker installation files. If you are using some other method to push the worker out to the workstations, or if you plan to copy either of the two worker installation *.msi files, sharing the Supervisor folder is not necessary.

NEW WORKER INFORMATION FOR THE DNA 3.5 RELEASE

Workers are now installed with an *.msi file rather than the old WorkerInstall.exe. There are two such files:

For 32-bit systems:

AccessData DNA Worker.msi

OR

For 64-bit syterms:

AccessData DNA Worker (64-bit).msi

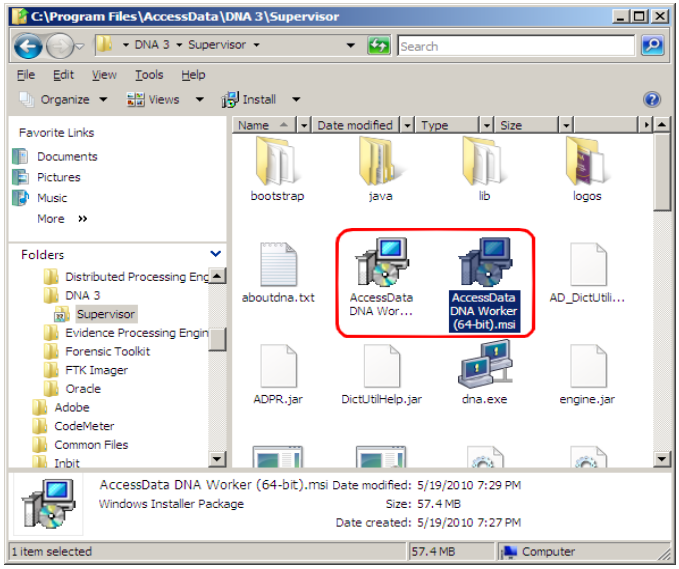
To install the worker on a Windows workstation, do the following:

New workers update via Group Policy when the worker machine is rebooted. If you do not use Windows Server 2003, or do not implement Group Policies, do the following to install your workers:

1. On the Windows workstation, browse to the shared Supervisor directory and do one of the following:
   - Double-click the correct *.msi file on the Supervisor machine, file as explained above
   - Copy the correct *.msi file to the local worker machine, and execute it there.
   - Right click on the correct *.msi file and choose *Install*.

- Push the worker out to the worker computers using a third party product such as a Windows Server Group Policy.

Figure 2-1 Location of the WorkerInstall.msi File



2. Click *Next* on the Welcome screen.

AccessData DNA Worker - InstallShield Wizard
Welcome to the InstallShield Wizard for AccessData DNA Worker
The InstallShield(R) Wizard will install AccessData DNA Worker on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

3. Click *Yes* to accept the license agreement, then click *Next*.
4. If using Windows Vista, approve the installation.
5. Click *Next* on the Supervisor Information screen.

Important: Do not change any of the values, unless you want to connect this worker to a different supervisor.

6. On the Ready to Install screen, click *Install* to proceed with the worker installation.
7. Click *Next* on the screens as they appear, after reading their content.
8. When the installation is complete, Click *Finish* to finalize and close the worker installation wizard.

   After the installation is completed the worker service runs and connects to the Supervisor.

   When you execute the Worker.exe file found in the Supervisor folder, the Worker Status icon appears in the Taskbar. Clicking the Worker Status icon opens the DNA Worker Status screen. For more information about the DNA Worker Status screen, see "Understanding the DNA Worker Interface" on page 57.

The worker interface shows workers that are older than the current version of DNA with a light red background.

Important: All workers will need to be updated to the latest version of the shipping build of DNA as there have been numerous changes which will not allow an older worker to process jobs. Any workers that were set up with a Beta version of 3.5 should also be updated.

DNA 3.3.4 and earlier workers will uninstall automatically when the new *.msi is run.

Worker update is accomplished through a Group Policy.

SETTING UP A GROUP POLICY

Workers should be set up on a domain that will allow a group policy to be utilized to push a newer version of the worker down to the specified machines.

A group policy should then be created from the domain server with the WorkerInstall.msi that will push the worker out to the existing or new clients.

Note: See Microsoft Group Policy instructions on how to set up the policy. There is a document on Microsoft's web site called "Introduction to Group Policy in Windows Server 2003" that gives a good overview of Group Policy.

WORKER INSTALLATION ON A MACINTOSH WORKSTATION

Important: When installing to Macintosh or Linux workstations, it is important that SCP and SSH are already available on those workstations to facilitate the worker installation from the Windows Supervisor machine.

Important: Note that all commands for Macintosh, Linux, and PS3 are case-sensitive. Type these commands exactly as written.

You can manually install the DNA Worker at the local machine or from the DNA Supervisor machine.

Installing a DNA Worker Locally on a Macintosh Workstation

To install the DNA Worker locally, complete the following steps as user root at a terminal on the target Macintosh machine.

If the SSH service on a Mac needs to be started, execute the command by starting a terminal on the Mac. Log in as root user and run:

```
./sbin/service ssh start
```

This will start the service and allow access to the Mac using SSH.

Sometimes the Mac requires the Root user to install/uninstall the program. If the error: "Operation not permitted." comes up, type: login root at the command line and provide the root password. Proceed as follows:

1. Copy worker-mac-install.sh from the Windows Supervisor folder to a folder on the Mac box using a command prompt:

   scp worker-mac-install.sh [*Mac box name*]:

   By default, the folder is copied to the /Users/[*username*] folder.
2. Once copied, logon to the box by typing ssh *user*@[*box_name*] and switch to the root user:

   2a. Login root.

   2b. Supply your password if prompted, and press *Enter*.
3. Change the directory to the folder containing the file worker-mac-install.sh: (should be cd /users/[*user_name*]) and run:

   ./worker-mac-install.sh
4. Once the worker is installed, go to the /opt/Accessdata/DNA3/Worker folder by typing:

   cd /opt/AccessData/DNA3/Worker
5. Run the following command to start the worker service:

   ./dna3workerd start
6. Once running, the worker on this Mac box should display the IP address and name of the machine on the Supervisor.

7. To stop the worker service run the following command:

   ./dna3workerd stop.

INSTALLING A DNA WORKER REMOTELY ON A MACINTOSH WORKSTATION

Before you remotely install the DNA Worker on a Macintosh machine, verify the following:

- The DNA Supervisor is already installed on a Windows machine.
- SCP and SSH command files are available on the supervisor and worker machines.
- The file copied from the supervisor folder to the Macintosh workstation by whatever means available.

  Note: The worker-mac-install.sh worker install file can also be copied to a USB thumb drive or CD, or using a third party utility designed for remote access by IP address.
- A user account on the Macintosh workstation.

To remotely install the DNA Worker from the supervisor machine:

1. Modify the Hosts file in C:\windows\system32\drivers\etc to include the IP address of the Macintosh worker machine.
2. At the worker terminal, copy worker-mac-install.sh from the Supervisor directory to a directory on the Macintosh machine:

   scp worker-mac-install.sh [*Macintosh machine name*]:

   By default, the file is copied to the /Users/[*username*] directory.
3. Login as root to the Macintosh workstation.

   3a. Type login root at the terminal and provide the root password.

   3b. Enter the user password for the Macintosh workstation.

   3c. Log in to the Macintosh workstation:

   \ssh *user*@[*machine_name]*

   You may need to start the ssh service. Start a terminal on the Macintosh. While logged in as root user, run

   /sbin/service ssh start
4. Go to the directory containing worker-mac-install.sh; type the following:

   ./worker-mac-install.sh
5. To change to the folder where the worker service file is located, type:

   cd /opt/Accessdata/DNA3/Worker
6. To start the worker service, run the following command:

   ./dna3workerd start

The worker runs on the Macintosh workstation and displays the IP address and machine name of the supervisor.

Note: If you get a library error when trying to start the worker, then go to the /opt/Accessdata/DNA3/Worker directory and type the following:

```
DYLD_LIBRARY_PATH=. sh ./dna3worker-mac start
```

7. To stop the worker service, run the following command:

```
./dna3workerd stop
```

8. To check the status of the worker service, run the following command:

```
./dna3workerd status
```

WORKER INSTALLATION ON A LINUX WORKSTATION

The versions of Linux that are supported for DNA workers are as follows:

- Fedora Core 11
- Fedora Core 12

When installing to Linux-based workstations, it is helpful that SCP and SSH are already available on those workstations to facilitate the worker installation from the Windows Supervisor machine.

Important: Note that all commands for Linux-based boxes are case-sensitive. Type these commands exactly as written.

You can install the DNA Worker on the local machine or from the DNA Supervisor machine. Modify the hosts file under C:\windows\system32\drivers\etc to include the IP addresses of the worker machines so you can log on to the correct box and use the SCP and SSH commands for file transfer.

INSTALLING A DNA WORKER LOCALLY ON A LINUX WORKSTATION

To install the DNA Worker locally, complete the following steps as user root at the command line on the target Linux machine:

1. Copy the correct install file from the Windows Supervisor folder to a folder on the Linux box using any means available. The two files are as follows:

   For 32-bit:

   worker-i386-install.sh

   OR

   For 64-bit:

   worker-amd64-install.sh

2. At the prompt on the Linux box, type the following command:

   scp worker-i386-install.sh [*Linux box name*]:

   OR

   scp worker-amd64-install.sh [*Linux box name*]:

   You will be prompted for your user password. By default, the folder is copied to the /Home/[*username*] folder.

3. Once copied, logon to the box by typing ssh user@[*box_name*] and switch to the root user:

   su (prompts for password, if applicable)

4. Change directory to the folder you copied worker-i386-install.sh or worker-amd64-install.sh to:

   cd /home/[*user_name*]

   4a. Run:

   ./worker-i386-install.sh

5. When prompted to install Java, click *Yes*.
6. Once Java is installed, go to the /opt/Accessdata/DNA3/Worker folder by typing:

   cd /opt/AccessData/DNA3/Worker

7. Run the following command to start the worker service:

   ./dna3workerd start

8. Once running, the worker on this Linux box should display with the IP address and name of the Supervisor machine.
9. Run the following command from the AccessData folder to stop the worker service:

   ./dna3workerd stop

10. To check the status of the worker service, run the following command:

    ./dna3workerd status

INSTALLING A DNA WORKER REMOTELY ON A LINUX WORKSTATION

Before you remotely install the DNA Worker on a Linux machine, verify the following:

- The DNA Supervisor is already installed on a Windows machine.
- Scp and ssh command files are available on the supervisor machine.
- You have a user account on the Linux machine.

To remotely install the DNA Worker from the supervisor machine:

1. Modify the Hosts file in C:\windows\system32\drivers\etc to include the IP address of the worker machine.

2. Using a command prompt, copy worker-i386-install.sh or worker-amd64-install.sh from the Supervisor directory to a directory on the Linux machine:

   scp worker-i386-install.sh [*Linux_machine_name*]:

   OR

   scp worker-amd64-install.sh [*Linux_machine_name*]:

   By default, the folder is copied to the /home/[*username*] directory.
3. Enter the user password for the Linux machine.
4. Log in to the Linux machine:

   ssh user@[*machine_name]*
5. Switch to the root user:

   su
6. (Conditional) Enter the root user password.
7. Go to the directory in which you copied worker-i386-install.sh or worker-amd64-install.sh; type the following:

   ./worker-i386-install.sh

   OR

   ./worker-amd64-install.sh
8. When prompted to install Java, click *Yes*.
9. After Java is installed, go to the /opt/Accessdata/DNA3/Worker directory:

   cd /opt/AccessData/DNA3/Worker
10. To start the worker service, run the following command:

    ./dna3workerd start

    The worker on the Linux machine displays the IP address and machine name of the supervisor.
11. To stop the worker service, run the following command:

    ./dna3workerd stop
12. To check the status of the worker service, run the following command:

    ./dna3workerd status

DNA Worker Installation on a Sony Playstation 3 (PS3)

To install the DNA Worker on a Sony Playstation 3 (PS3), complete the following steps as user root at the command line on the target Linux machine:

TO INSTALL A PS3 WORKER:

Prior to worker installation you must have either OpenSuSE 11 Power-PC or Ubuntu 8.10 installed as the active operating system on the PS3 box. If you have problems with the OpenSuSE 11 or Ubuntu 8.10 installation, please refer to specific documentation for that product. AccessData does not offer support for third party software.

For firmware version 2.51, install OpenSuSE 11. For firmware version 2.52 or later, install Ubuntu 8.10 or later.

Installing the DNA worker:

1. scp worker-ppc32-install.sh *[PS3 box name]*: directory on the PS3.

   You will be prompted for your user password.

   By default, the folder is copied to the /home/[*username*] folder.
2. Once copied, logon to the box by typing ssh user@[*box_name*] and switch to the root user:

   su (prompts for password, if applicable).
3. Change directory to the folder you copied worker-powerpc-install.sh to, such as:

   cd /home/[*user_name*]
4. Install the worker by running:

   sh worker-ppc32-install.sh install
5. Go to the /opt/Accessdata/DNA3/Worker folder by typing:

   cd /opt/AccessData/DNA3/Worker.
6. Run the Worker by typing:

   ./dna3workerd start

   Once running, the worker on this PS3 box should display the IP address and name of the worker machine connected to the Supervisor.
7. To stop the worker service, run the following command:

   ./dna3workerd stop
8. To check the status of the worker service, run the following command:

   ./dna3workerd status

To stop the worker service:

Run the following command from the AccessData folder to stop the worker service:

./dna3workerd stop

Should you need to uninstall the worker:

1. From the /opt/AccessData.DNA3/Worker directory, run:

   ./dna3workerd stop

2. Change to the /Home/[username] directory.
3. Type:

   sh worker-ppc32-install.sh uninstall

For more information regarding uninstalling other DNA workers, see "Uninstalling the DNA Worker" on page 28.

AFTER INSTALLING PRTK OR DNA

Before running PRTK or DNA, you must install a dongle and the dongle drivers, and add licenses to the dongle. For more information, see "PRTK or DNA Installation Prerequisites" on page 8.

LICENSING

You can manage product licenses on a dongle using LicenseManager.

For information about installing LicenseManager, see "Installing LicenseManager" on page 12.

For information about starting LicenseManager, see "Chapter 10 Managing Security Devices and Licenses" on page 147.

UNINSTALLING PRTK OR DNA

The following sections will guide you through uninstalling PRTK, or a DNA Supervisor and/or its workers.

UNINSTALLING PRTK

You can uninstall PRTK just as you would typically remove other programs from the Windows Control Panel.

To uninstall the PRTK program:

1. Under the Start menu, select *Control Panel* > *Add or Remove Programs*.
2. Select *AccessData PRTK 6*; then click *Remove*.

3. Select *Uninstall PRTK 6*; then click *Next*.
4. Click *Yes* to proceed with the uninstall.
5. Click *Finish* to complete the uninstall.

Important: After the uninstall is complete, there are still some files left on your computer. Go to [*drive*]:\Documents and Settings\All Users\Application Data\AccessData\PR to see these files. You may wish to keep these files, or if the computer will no longer be used for password recovery, delete the \PR\ folder to complete the uninstall.

To uninstall the CodeMeter Runtime software if no other AccessData products are installed or to be installed on this computer:

1. Under the Start menu, select *Control Panel* > *Add or Remove Programs*.
2. Select the *CodeMeter Runtime Kit v3.30a*, then click *Change/Remove*.
3. Click *OK* to proceed with the uninstall.
4. Click *Finish* to complete the uninstall.

To uninstall the dongle drivers if they are no longer necessary for other programs on this computer:

1. Under the Start menu, select *Control Panel* > *Add or Remove Programs*.
2. Select the *AccessData Dongle Driver*; then click *Change/Remove*.
3. Click *OK* to proceed with the uninstall.
4. Click *Finish* to complete the uninstall.

UNINSTALLING THE DNA SUPERVISOR

You can uninstall the DNA Supervisor from the Windows Control Panel. You can perform one of the following:

- Partial uninstall: Removes the DNA program files. You can select a partial uninstall if a program file becomes corrupted. You can then re-install the supervisor without losing your customized DNA files, such as profiles, rules, and the communication keys. For more information, see "Supervisor Installation" on page 13.
- Full uninstall: Removes all files in the Supervisor directory, including program files and customized files. If you perform a full uninstall, the workers subordinate to the supervisor stop processing jobs, unless you back up the supervisor keys first.

  To backup the supervisor keys, refer to "Backing Up and Restoring Keys" on page 54.

To uninstall the DNA Supervisor:

1. Under the Start menu, select *Control Panel* > *Add/Remove Programs*.
2. Select *AccessData DNA 3 Supervisor* and click *Change/Remove*.
3. Select the desired type of uninstall and click *Next*.
4. Click *Finish*.

Important: After the uninstall is complete, there are still some files left on your computer. Go to [*drive*]:\Documents and Settings\All Users\Application Data\AccessData\PR to see these files. You may wish to keep these files, or if the computer will no longer be used for password recovery, delete the \PR\ folder to complete the uninstall.

To uninstall the CodeMeter Runtime software if no other AccessData products are installed or to be installed on this computer:

1. Under the Start menu, select *Control Panel* > *Add or Remove Programs*.
2. Select the *CodeMeter Runtime Kit v3.30a*, then click *Change/Remove*.
3. Click *OK* to proceed with the uninstall.
4. Click *Finish* to complete the uninstall.

To uninstall the dongle drivers if they are no longer necessary for other programs on this computer:

1. Under the Start menu, select *Control Panel* > *Add or Remove Programs*.
2. Select the *AccessData Dongle Driver*; then click *Change/Remove*.
3. Click *OK* to proceed with the uninstall.
4. Click *Finish* to complete the uninstall.

UNINSTALLING THE DNA WORKER

You can uninstall the DNA Worker from Windows workstations and from Macintosh, Linux, and PS3 machines.

UNINSTALLING THE DNA WORKER ON A WINDOWS WORKSTATION

You can uninstall the DNA Worker from the Windows Control Panel.

To uninstall the DNA Worker:

1. Under the Start menu, select *Control Panel* > *Add/Remove Programs*.
2. Select *AccessData DNA 3 Worker* and click *Change/Remove*.

If you are prompted that the application is still running, right-click the key icon in the Taskbar and select *Exit*.

3. Click *OK* to remove the DNA worker and all its components.
4. Click *Finish*.

To Uninstall a Linux, Mac, or PS3 Worker

To uninstall the DNA Worker on a Mac, Linux, or PS3 machine, complete the following steps as user root at the command line:

1. Go to the /opt/Accessdata/DNA3/Worker directory.
2. Stop the worker service by typing the following:

   ./dna3workerd stop
3. Press Enter
4. Run the install *.sh file from the folder you copied it to with the additional 'uninstall' switch, as follows:

TABLE 2-1 Uninstall Commands for Linux, Mac, and PS3

Operating System	Command to Type
Linux	./worker-i386-install.sh uninstall
Mac	./worker-mac-install.sh uninstall
PS3	./worker-powerpc-install.sh uninstall

For example:

4a. On a Macintosh workstation, type:

sh worker-mac-install.sh uninstall

OR

./worker-mac-install.sh uninstall

4b. On a Linux-based machine, type:

sh worker-i386-install.sh uninstall

OR

./worker-i386-install.sh uninstall

4c. On a PS3 machine, type:

sh worker-powerpc-install.sh uninstall

OR

./worker-powerpc-install.sh uninstall

This command will remove the AccessData/DNA3/Worker directory and the related symbolic links.

Note: The ./worker... accomplishes the same thing as sh worker...

UNINSTALLING THE SECURITY DEVICE DRIVERS

You can uninstall the Wibu CodeMeter software if no other AccessData products are installed on this machine, and you can uninstall the Keylok dongle driver if no other AccessData programs rely on it for license information.

Both security device drivers can be uninstalled from the Windows Control Panel.

To uninstall the Wibu CodeMeter software:

1. On the supervisor machine, click *Start* > *Control Panel* > *Add/Remove Programs*.
2. Select *CodeMeter Runtime Kit v3.30a* and click *Change/Remove*.
3. Click *OK* to remove the CodeMeter software and all its components.
1. Click *Finish*.

To uninstall the dongle driver:

1. On the supervisor machine, select *Control Panel* > *Add/Remove Programs*.
2. Select *AccessData Dongle Driver* and click *Change/Remove*.
3. Click *OK* to remove the dongle driver and all its components.
4. Click *Finish*.

Chapter 3 Getting Started

This section acquaints you with the basic features of both AccessData® Password Recovery Toolkit® (PRTK®) 6.5 and AccessData Distributed Network Attack® (DNA®) 3.5.

STARTING PRTK OR DNA

To run PRTK, select *Start* > *All Programs* > *AccessData* > *PRTK 6* > *PRTK.exe*.

OR

Click the *PRTK* desktop shortcut .

To run DNA, click *Start* > *All Programs* > *AccessData* > *Distributed Network Attack* > *Supervisor.exe*.

OR

Click the *Supervisor* desktop icon .

When starting, PRTK and DNA search for a license. If you do not have a CmStick or a dongle or if the CodeMeter software or the device drivers are not installed correctly, then the product runs in demo mode, allowing you to run decryption jobs on a limited number of file types. For more information, see, "Running PRTK or DNA in Demo Mode" on page 32.

PRTK and DNA use services to handle password recovery functions. The services must be running for PRTK to successfully do its job.

Typically, the services are started when PRTK is started, and the services are stopped when PRTK is stopped.

When DNA is installed, the services start automatically and continue to run, even when the User Interface is closed.

If PRTK or DNA does not start properly, see "Chapter 11 Troubleshooting" on page 173.

Using the USB Security Device

Typically, AccessData product licenses reside on the same CodeMeter stick or dongle. This configuration assumes that you are running the products on a single machine. (You can use only one AccessData security-compliance device at a time on any one computer.) If you prefer to run the products on separate machines, you can order an additional CmStick for a nominal fee. For more information, contact AccessData at www.accessdata.com, or contact your AccessData Sales Representative.

Note: Running FTK, PRTK or DNA, and the Registry Viewer on a single machine facilitates interaction between the products. For example, FTK 2.1 and above has an option to automatically decrypt EFS files using PRTK. As long as FTK and PRTK licenses are on the same dongle, and the dongle and the products are installed on the same machine, PRTK automatically decrypts these files for FTK. If you run the products on different machines, you lose some of this integrated functionality. Keep in mind, however, that running them on the same machine may heavily tax the resources of that machine.

Use LicenseManager to manage your product licenses once the CmStick and the CodeMeter software, or the CodeMeter software, the dongle device drivers and the dongle are installed on your decryption computer. For more information, see "Chapter 10 Managing Security Devices and Licenses" on page 147.

Running PRTK or DNA in Demo Mode

When you run PRTK or DNA without a security device, you can run only the demo version of the product. This limits the types of files you can run attacks on.

The demo version includes the following modules:

- Zip Dictionary Attack
- Old Format PGP Secret Key Ring Dictionary Attack
- PGP Disk 4.0/5.0/6.0 Dictionary Attack
- PGP® Secret Key Ring Dictionary Attack

RIGHT-CLICK MENUS

Throughout the interface you can right-click the mouse to see features specific to the context of the tasks you are performing.

VIEWING MODULE INFORMATION

You can view information about password recovery modules, including information about module names, display names, attack types, and supported products and versions.

To view module information, click *Help* > *Recovery Modules*.

CUSTOMIZING THE USER INTERFACE

The PRTK interface consists of the Menu bar, the Tool bar, the Job Queue pane, and the Properties pane. DNA has an additional pane, the Priority Groups pane.

You can customize several aspects of the interface to fit your needs or preferences. All windows and dialogs are resizeable in this version of PRTK and DNA. However, the resized windows are not persistent, meaning that after resizing the window, once closed, the next time that window is opened, it will be the default size.

If you make changes to the view and want to quickly reset it to the default, click *View* > *Reset Views*.

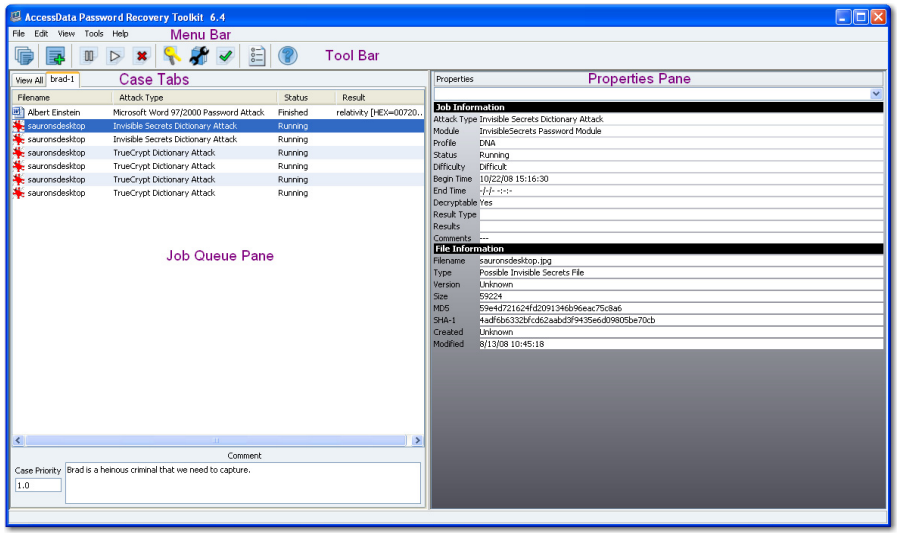
SHOWING OR HIDING ELEMENTS

You can show or hide the Toolbar, Properties Pane, and Priority Groups Pane (DNA).

To show or hide an element of the user interface, click View. Select an element to toggle an item in the view. This places a check mark next to the element you selected, indicating that the element is displayed in the view. To turn off or remove an element from the view, click View, then select the element to remove it from the view. This

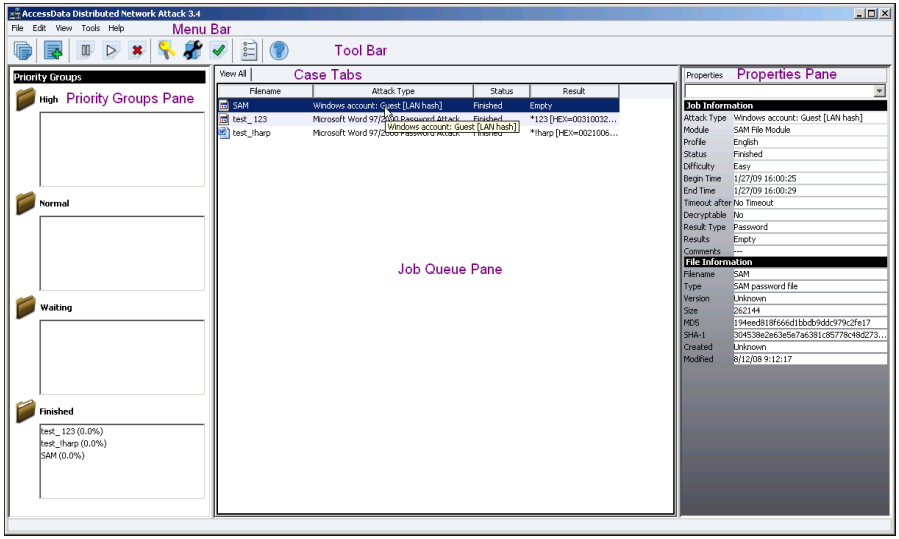
removes the check mark next to that element, indicating that it is not being displayed in the view.

Figure 3-1 The PRTK Interface



The DNA interface is essentially the same as the PRTK interface, with the addition of the Priority Groups Pane, as seen in the following figure:

Figure 3-2 The DNA Interface



THE MENU BAR

The Menu Bar above the Tool Bar lets you access product features.

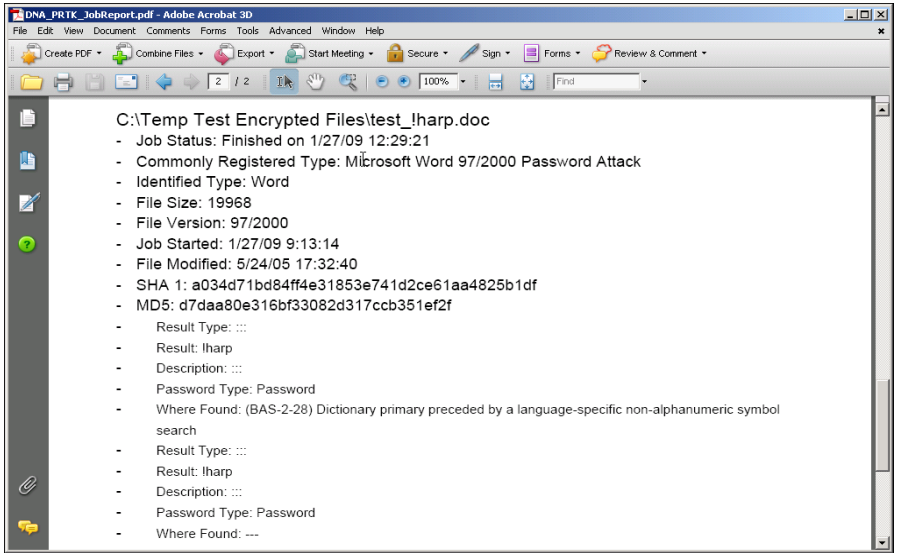
The following tables provide information about the various Menu Bar items, and their descriptions.

The File Menu contains the following options:

TABLE 3-1 File Menu Items

Menu Item	Description
New Case	Create a new case. This allows you to keep files from one case together, or from several cases separate from each other.
Delete Case	Delete an existing case.
Add Files	Add files to be processed.
Pause All	Pause all jobs. To pause an individual job, right-click on the job, and choose *Pause*.
Resume All	Resume all paused jobs. To resume an individual job, right-click on the job and choose *Resume*.
Delete All	Delete all jobs. To delete a single job, right-click on the job and choose *Delete*.
Connect	Connect to the supervisor service.
Disconnect	Disconnect from the supervisor service.
Generate Report	Generate a job report in .PDF format. See the figure following this table for the information contained in the report.
Exit	Exits the program. When exited, PRTK terminates the services, but saves the jobs it was working on until the next time the program is run. DNA does not terminate the services, and they can continue to run in the background on worker machines.

Figure 3-3 Generated Report Statistics


DNA_PRTK_JobReport.pdf - Adobe Acrobat 3D
File Edit View Document Comments Forms Tools Advanced Window Help
Create PDF Combine Files Export Start Meeting Secure Sign Forms Review & Comment
C:\Temp Test Encrypted Files\test_!harp.doc
- Job Status: Finished on 1/27/09 12:29:21
- Commonly Registered Type: Microsoft Word 97/2000 Password Attack
- Identified Type: Word
- File Size: 19968
- File Version: 97/2000
- Job Started: 1/27/09 9:13:14
- File Modified: 5/24/05 17:32:40
- SHA 1: a034d71bd84ff4e31853e741d2ce61aa4825b1df
- MD5: d7daa80e316bf33082d317ccb351ef2f
- Result Type: :::
- Result: !harp
- Description: :::
- Password Type: Password
- Where Found: (BAS-2-28) Dictionary primary preceded by a language-specific non-alphanumeric symbol search
- Result Type: :::
- Result: !harp
- Description: :::
- Password Type: Password
- Where Found: ---

The Edit Menu contains the following options:

TABLE 3-2 Edit Menu Items

Menu Item	Description
Rules	Opens the Rules editor.
Profiles	Opens the Profiles editor.
Select All	Select all jobs in the Job Queue Pane.
Preferences	Opens the Preferences view with its three tabs (PRTK) or four tabs (DNA). The Preferences tabs are as follows: • General • Audio Alerts • Drop Folder • Worker (DNA Only) See the section "Changing Preferences" on page 39 for more detailed information.
Network License Information	If you are running PRTK or DNA using a Network License, that information is available here.

The View Menu contains the following options:

TABLE 3-3 View Menu Items

Menu Item	Description
Toolbar	Shows or hides the Toolbar.
Properties Pane	Shows or hides the Properties Pane.
(DNA) Priority Groups	Shows or hides the Priority Groups Pane. For more information regarding the Priority Group Pans, see "Priority Groups Pane" on page 49.
File Properties	Opens the Properties View for the selected job. There are three tabs in this view: • Information • Rules • Passwords/Second
(DNA) Workers Information	Opens the Workers Information View.
Reset Views	Resets the Views to the default settings.

The Tools Menu contains the following options:

TABLE 3-4 Tools Menu Items

Menu Item	Description
Dictionary Tools	Opens the Dictionary Tools interface, making all dictionary options available.
(DNA) Backup Keys	Creates a backup of the keys necessary for the Supervisor/ Worker Communication.
(DNA) Restore Keys	Restores from the backup file the keys necessary for the Supervisor/Worker Communication.
(DNA) Stop Supervisor	Stops the DNA Supervisor service.
(DNA) Start Supervisor	Starts the DNA Supervisor service.

The Help Menu contains the following options:

TABLE 3-5 Help Menu Items

Menu Item	Description
Contents	Opens the PRTK (& DNA) User Guide.

TABLE 3-5 Help Menu Items

Menu Item	Description
Online Support	Opens the AccessData Website to the Support Page where you can easily find a variety of AccessData product support information.
Recovery Modules	Opens a view of the up-to-date listing of the Recovery Modules available for this version at the time of release.
About PRTK 6.5 or DNA 3.5	Opens a view of the specific version and copyright information for this release of the product.

CHANGING PREFERENCES

To access the Preferences page, click *Edit* > *Preferences*. You will see four tabs:

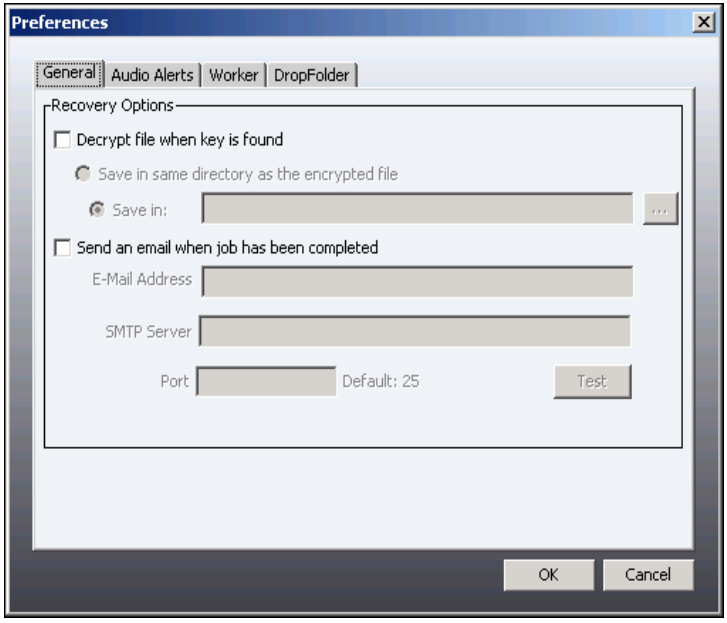
- General
- Audio Alerts
- (DNA) Worker
- DropFolder

These tabs are covered in detail below:

GENERAL TAB

The General tab provides the following Recovery Options, as illustrated in the figure below:

Figure 3-4 Job Preferences General Tab:



SPECIFYING RECOVERY OPTIONS

You can set default recovery settings to use when processing jobs in the recovery session. By default, the program does not automatically decrypt a file after a key is discovered. You can choose to have the key automatically applied to the file, and you can receive an email when the job is completed. You can configure both these features in the Recovery Options section of the Preferences form.

DECRYPT FILE WHEN KEY IS FOUND

Allows you to specify a location the same as or different from where the original file was stored when it was added to DNA. If saved in the same folder, the word "decrypted" will be appended to the file name.

To automatically decrypt the file after a key is found:

1. Select *Edit* > *Preferences.* > *General.*

2. Check the *Decrypt File When Key Is Found* box.
3. Select *Save in Same Directory as the Encrypted File*, or select *Save In* and browse to and select the desired directory.

   The directory of the encrypted file is the directory that you added the encrypted file from using the Add Job Wizard, or the folder you dragged and dropped the file from when you added it to the Job Queue. You might want to specify a different directory if you want to keep all decrypted files in one location.

   Note: After a file is decrypted with a key, the filename is appended with *-decrypted*: for example, file1-decrypted.xls.
4. Click *OK*.

SAVING DECRYPTED FILES MANUALLY

After PRTK recovers the decryption key of a file, you can manually decrypt and the decrypted file will be saved automatically.

To decrypt a file after recovering the key:

1. In the PRTK window, right-click a job that has a recovered decrypt key.
2. Select *Decrypt* from the menu.
3. Specify where to save the decrypted file.

SEND AN EMAIL WHEN JOB HAS BEEN COMPLETED

Allows you to specify whether to send an email when a job is completed, and to specify the address and details of where that email should be sent.

To receive an email after a job is completed:

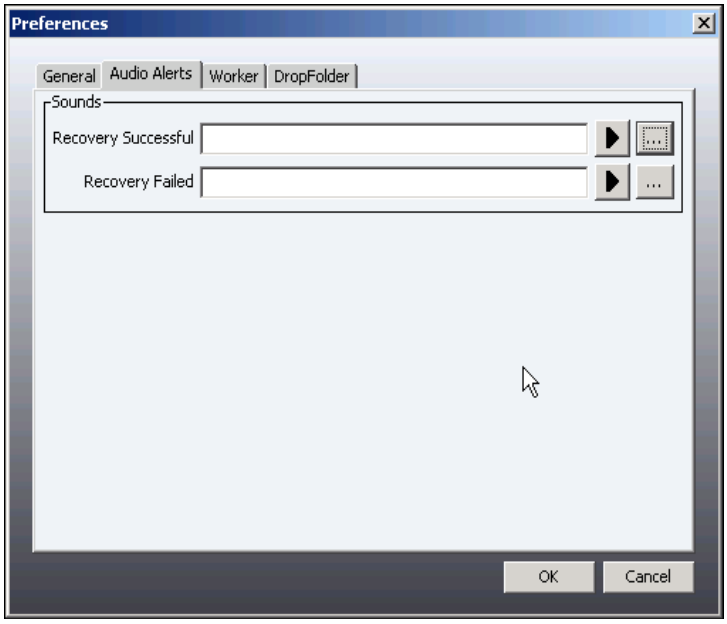
1. Select *Edit* > *Preferences* > *General*.
2. Check the *Send an Email When Job Has Been Completed* box.
3. In the Email Address field, enter the recipient's email address.
4. In the SMTP Server field, enter the name of the SMTP server for the specified email address.
5. In the Port field, enter the port number.
6. Click *Test* to send a test email to verify that the email address and SMTP server information is working.
7. Click *OK*.

Important: Sending an email works only with servers not requiring SMTP authentication.For an explanation of encrypted files, see "Understanding Encrypted Files" on page 217.

AUDIO ALERTS TAB

As shown in the following figure, the Audio Alerts tab provides options to specify a particular sound upon successful password or key recovery, and a different one upon a failed password or key recovery. Simply type in, or browse to the sound files to use.

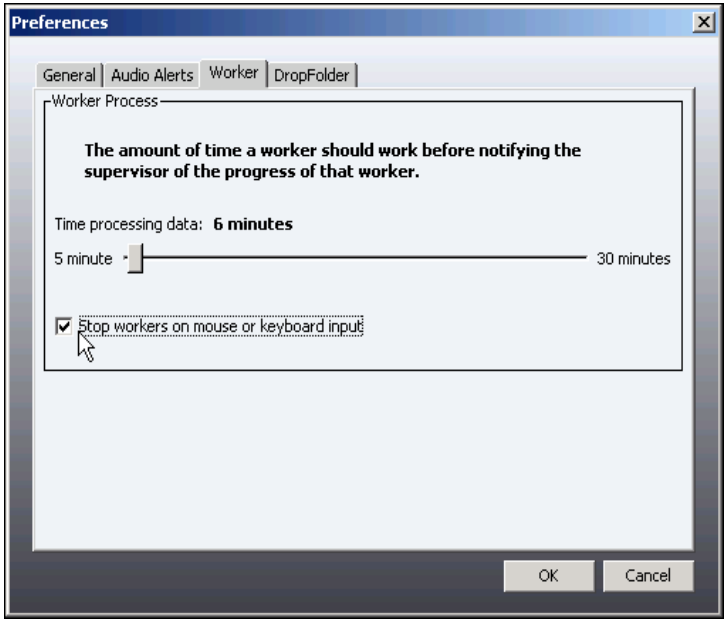
Figure 3-5 Setting Audio Alerts for Successful Recoveries



WORKER TAB (DNA)

The Worker tab (DNA) gives you control over the amount of time the worker should work before updating its progress to the Supervisor, and allows you to set the option for "Stop workers on mouse or keyboard input".

Figure 3-6 Setting Worker Preferences



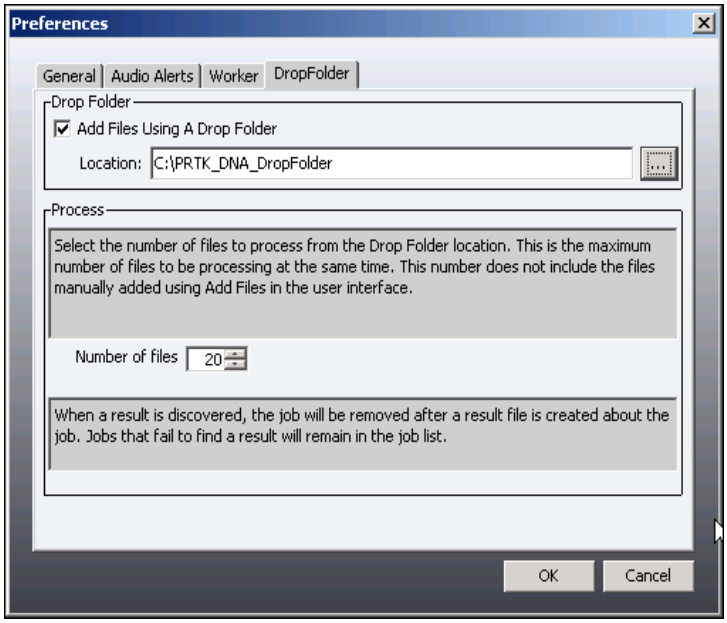
If you are setting workers up on systems where employees normally work during the day, for example, selecting this option prevents jobs from being processed during the times when the employee would be doing normal work. Each time mouse or keyboard input is detected, the worker is suspended for approximately 10 minutes, then resumes if no further activity is detected.

DROPFOLDER TAB

The DropFolder tab gives you the option of setting up a dropfolder for adding jobs. The dropfolder will be monitored by DNA and jobs are processed in the order they are

added to the dropfolder. When jobs are completed, they will be placed according to the options you selected under the General preferences tab.

Figure 3-7 Setting Preferences on the General Tab


Preferences
General
Audio Alerts
Worker
DropFolder
Drop Folder
Add Files Using A Drop Folder
Location:
C:\PRTK_DNA_DropFolder
Process
Select the number of files to process from the Drop Folder location. This is the maximum number of files to be processing at the same time. This number does not include the files manually added using Add Files in the user interface.
Number of files
20
When a result is discovered, the job will be removed after a result file is created about the job. Jobs that fail to find a result will remain in the job list.
OK
Cancel

In addition to setting up the dropfolder, you can specify the maximum number of files to be processing at the same time that have been added through using the dropfolder. This number does not include files added by drag and drop or using the *Files* > *Add Files* menu or the *Add Files* button.

THE TOOLBAR

The Toolbar provides easy access to various functions in PRTK and DNA.

Figure 3-8 The PRTK and DNA Toolbar

The following table shows each Toolbar icon and describes its function:

TABLE 3-6 Toolbar Icons and Functions

Toolbar Icon	Function
	Generate a Report for the current recovery session.
	Select files to add to the recovery session.
	Pause All Jobs. To pause a single job, select one job and right-click. Click *Pause*.
	Resume All Jobs. To resume a single job, select one job and right-click. Click *Resume*.
	Delete All Jobs. To delete a single job, select one job and right-click. Click *Delete*.
	Manage Profiles.
	Open Dictionary Tools.
	Verify Hashes.
	Access Preferences.
	Open Help Topics.

THE JOB QUEUE PANE

The PRTK and DNA Job Queue pane displays the files that are being processed in the current session, along with some of their individual file attributes.

The following table describes all columns in the Job Queue pane:

TABLE 3-7 Job Queue Pane

Group	Description
Filename	The complete name of the encrypted file, including the full path to the file and the file extension.

TABLE 3-7 Job Queue Pane

Group	Description
Attack Type	The attack type used to decrypt the file. The following are the possible attack types: • Dictionary • Decryption • Keyspace • Reset If DNA is using either the dictionary or keyspace attack, more specific information is listed about the type of attack being used. For more information on the attack types, see"Understanding the PRTK & DNA Decryption Process" on page 218.
Status	Current status of the Job in the Queue. Possibilities are: • Running • Waiting • Depends_on • Finished
Result	The result of the completed job. An asterisk (*) indicates multiple passwords were found, such as both Open and Modify, for a single job. Double-click the Job in the Job Queue Pane to see the Job Properties and Results in more detail.

JOB PROPERTIES

Double-click or right-click on a job and select *File Properties* to open the Properties view of the highlighted job file.

Three Tabs display:

- **Information**: displays file name, file information, job properties, and job results.
- **Rules**: displaying the percentage of the job Rules that are unassigned, assigned, completed, or failed.
- **Passwords/Second**: displays a graph indicating the number of passwords being tried per second. The graph updates every 60 seconds. This setting is not user-configurable.

Comments displayed must be added when the job is added to note specific points of interest for this job. If you try to add comments to a job that is running, when the

screen is refreshed, the comments field is cleared, so there is no way to save changes made here once the job is added.

The following Buttons are available on all tabs:

- **Apply**: Click *Apply* to save changes to the Rules tab, specifically when marking or unmarking either *Logarithmic* or *Automatic Refresh*.
- **Cancel**: Click *Cancel* to close any dialog without saving.
- **OK**: Click *OK* to close the dialog.

CHANGING ATTRIBUTES ORDER IN THE JOB QUEUE PANE

PRTK and DNA allow you to determine in what order the attributes appear in the Jobholder Pane. Simply click on an attribute column heading and drag it to the left or right until it is in the position you prefer, then release the mouse button.

Changing the Sort Order in the Job Queue Pane.

PRTK and DNA let you sort files by their file properties.

SIZING COLUMN HEADINGS IN THE JOB QUEUE PANE

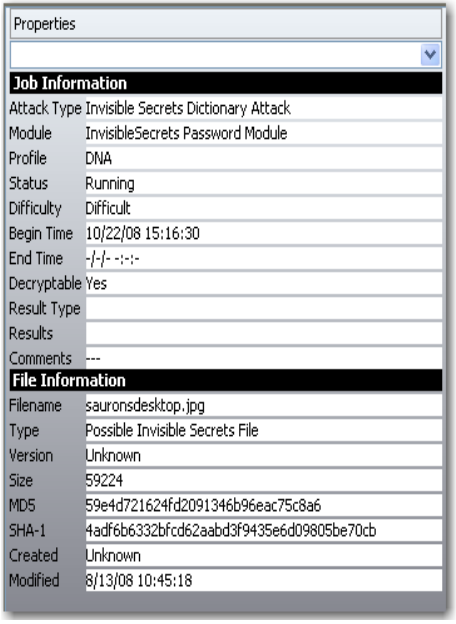
You can resize the columns in the PRTK or DNA Job Queue Pane.

To resize a column heading, allow the mouse cursor to hover over the separator between column headings until it changes to a double-arrow. Click and drag a column heading separator until the column width suits you.

THE PROPERTIES PANE

The Properties Pane shows available attributes of the selected file in the Job Window.

Figure 3-9 The Properties Pane



The following table describes the file attributes listed in the Properties Pane for a selected file:

TABLE 3-8 Properties Pane Attributes and Descriptions

Attribute Name	Attribute Description
Job Information	
Filename	Path and filename of the file
Attack Type	Attack type based on password recovery or decryption method (decryption or dictionary)
Module	Name of password recovery module
Profile	Name of profile used with job
Status	Status of the password recovery process (finished, running, depends on, paused, waiting)
Difficulty	Easy, moderate, or difficult password recovery

TABLE 3-8 Properties Pane Attributes and Descriptions

Attribute Name	Attribute Description
Begin Time	Start time of recovery process
End Time	End time of recovery process
Decryptable	Decryption method can be used on file
Result Type	Type of result
Results	Results of the password recovery
Comments	Specific comments you entered about the file when adding the job
File Information	
Filename	Path and filename of the file
Type	File type based on analysis of file
Version	Version of source application based on analysis of file
Size	File size
MD5	MD5 (128-bit) hash of the file contents
SHA-1	SHA (160-bit) hash of the file contents
Created	Date and time file was created
Modified	Date and time file was last modified

To view more attributes, double-click the selected file. See "Monitoring Jobs" on page 75.

DNA USER INTERFACE

When DNA is installed, there are some additional features, with few differences in the appearance of the User Interface. For more information regarding configuring DNA, see "Chapter 4 Managing DNA 3.5 System Configurations" on page 51.

The default management interface is divided into the Priority Groups Pane, the Job Queue Pane, and the Properties Pane.

PRIORITY GROUPS PANE

The Priority Groups Pane list is used to rank jobs by importance. The list displays the priority groups in DNA and the percentage of all available resources working on each priority. The priority of an active job can be changed between High and Normal,

however, Waiting and Finished jobs cannot be changed. The following table describes all groups in the Priority Groups list.

TABLE 3-9 DNA Priority Groups

Group	Description
High	The most urgent priority group for jobs in DNA. Jobs classified in this priority group are processed according to the order they are added to the group.
	By default, 90% of all available resources in the group or DNA system process jobs in the High Priority group, leaving 10% of resources to continue working on Normal Priority jobs.
Normal	The basic priority group in DNA. Jobs classified in this priority group are processed according to the order they are added to the group.
	By default, 10% of all available resources in the group or DNA system process jobs in the Normal Priority group.
Waiting	The group for jobs that are paused or waiting for another job to complete, or that have timed out.
	Jobs move out of this group after their processing is resumed.
Finished	The group that displays all processed jobs.

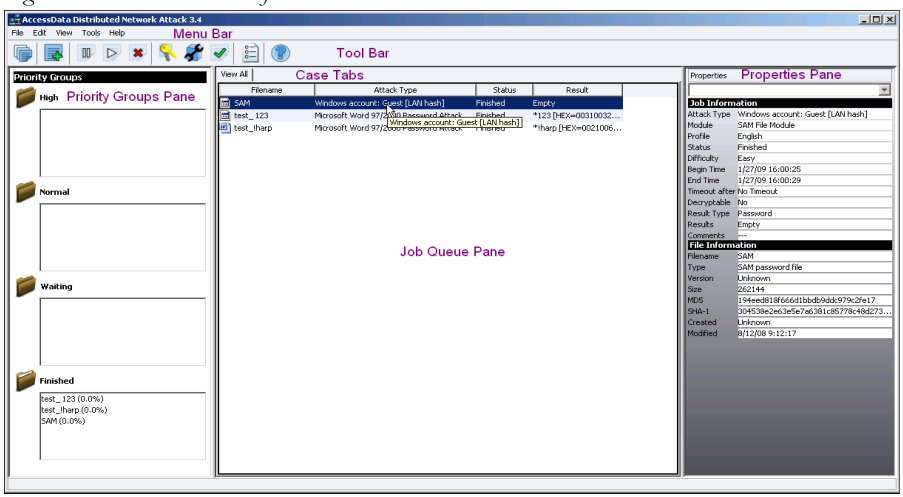
Chapter 4 Managing DNA 3.5 System Configurations

In PRTK, management tasks include defining Rules, Profiles, and Dictionaries, setting Preferences, and customizing the Interface.

DNA management tasks include the same tasks as in PRTK, but also include backing up the keys used for communication, managing Workers, and stopping or starting the Supervisor.

This chapter covers management tasks specific to DNA.

Figure 4-1 The DNA Interface



By default, the interface automatically displays Priority Groups, Jobs Queue Pane, and Properties of the currently highlighted jobs. If you make changes to the view and want to quickly reset it to the default, click *View* > *Reset Views*.

For information regarding customizing the User Interface, see "Customizing the User Interface" on page 33.

DISCONNECTING FROM AND CONNECTING TO THE DNA SERVICE

You might want to temporarily disconnect the DNA user interface from the DNA service to run maintenance procedures either on DNA, or on the machine itself.

To disconnect from the DNA service, select *File* > *Disconnect*.

After you finish the maintenance procedures, you must reconnect to the DNA service.

To connect to the DNA service, do the following:

1. Select *File* > *Connect*.
2. In the Login form, complete the following:

Figure 4-2 Entering the DNA Supervisor Login Information

3. In the Server field, enter the IP address of the DNA Supervisor machine.
4. In the Port field, enter the desired port number connection. The default port for the Supervisor is 49170.

STOPPING AND RESTARTING THE SUPERVISOR SERVICE

You can stop and restart the supervisor service. You might restart the supervisor service to refresh the workers' connection with it.

To stop the supervisor:

1. Click *Tools* > *Stop Supervisor*. DNA disconnects from the DNA service.

To restart the supervisor:

1. Click *Tools* > *Start Supervisor*. DNA connects to the DNA service.

RESTARTING THE WORKER

You can restart a DNA Worker to re-establish its connection. You might need to restart a worker if current statistics are not available in the Workers Information Pane.

Important: Do not restart the worker if you know it is currently processing jobs. If you restart the worker while it is processing a DNA job, then the work already completed on the job will be lost.

FROM THE SUPERVISOR USER INTERFACE

To restart a DNA Worker from the DNA Supervisor:

1. Click *View* > *Workers Information*.
2. Select the worker you want to restart.
3. Right-click and select *Restart*.

FROM THE WORKER INTERFACE

If the DNA Worker no longer displays in the Workers list and you know that the worker machine is running, you need to restart the DNA Worker from its machine, as explained below.

To restart a DNA Worker from the Worker machine:

1. On a Windows workstation, complete the following:
   1a. In the System Tray, right-click the *DNA Worker* icon and select *Open*.
   1b. Click *Restart*.

   OR

   Click S*tart* > *All Programs* > *AccessData* > *Distributed Network Attack* > *Worker*.
2. On a Macintosh or Linux machine, complete the following:
   2a. At the command line of the machine, go to the /opt/Accessdata/DNA3/Worker directory.
   2b. Type ./dna3workerd restart

Note: You must have administrator rights to restart a worker.

Backing Up and Restoring Keys

During the DNA Supervisor installation, a public and private key pair is generated. This key pair is used when a communications session is initiated between the DNA Supervisor and a DNA Worker. After the initial communication, a session key is created and used to secure communication for the rest of that session.

Backing Up Keys

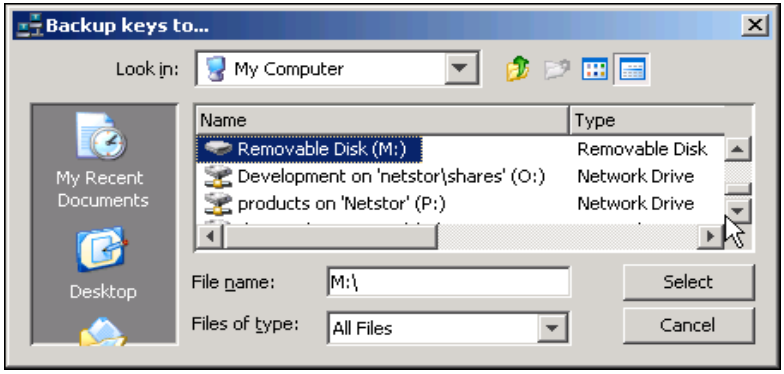
You can back up the key pair on the supervisor as a preventive measure against data loss. Backing up keys is also useful if you need to re-install the Supervisor.

Important: It is a good idea to backup the Supervisor Keys to either a network location or a removable media type. Doing so can save you from having to re-install every worker if a Supervisor re-install is necessary.

The backup keys can be restored to a Supervisor to maintain the communication with the current DNA Workers. If you re-install the supervisor without backing up and then restoring keys, the workers will be able to connect to the Supervisor but will not be able to process any jobs. In this case you must reinstall or update all the Workers before you can again process jobs.

You can use the backup keys for a partial installation of DNA. Before you start the installation, you must complete a partial un-install. If you perform a completely new install, new keys are created.

Figure 4-3 Backup Keys



To back up the keys:

1. Select *Tools* > *Backup Keys*.

2. Browse to and select the backup location for the keys; then click *Select*. The file supervisor.ini is saved to the selected location.

RESTORING KEYS

You can restore the key pair to the Supervisor if you experience a loss of data.

For example, if the entire system or a DNA Supervisor hard drive is lost, you can install a new version of DNA and restore the backup keys, assuming the backup was stored on a different system or a removable media type. As long as the hostname and IP address of the supervisor remains the same, the supervisors and workers do not have to change any configuration to work with the restored system.

To restore the keys:

1. Select *Tools* > *Restore Keys*.
2. Browse to and select the supervisor.ini; then click *Select*.

VIEWING WORKERS INFORMATION FROM THE SUPERVISOR MACHINE

The following table describes each component of the DNA Worker Information interface accessed by clicking *View* > *Workers Information*.:

TABLE 4-1 DNA Workers Information Screen

Component	Description
Hostname	Network recognized hostname of a worker on the DNA system.
IP Address	IP address of a worker on the DNA system
Processors	Number of processors available on this worker
Connected	Yes or No, depending on whether the DNA Worker is connected to the supervisor. Green indicates a connection, while red indicates that the worker is unavailable or disconnected.
Last Contact Time	The last date and time the supervisor contacted the DNA Worker.
Working On	Name of current job being processed.
Group Name(s)	Name(s) of the Group(s) this worker belongs to.

TABLE 4-1 DNA Workers Information Screen

Component	Description
Status Bar	At the bottom of the screen you will see information regarding • Connection status of the selected worker. Connected workers display in green in the list; non-connected workers display in red. • Number of workers connected vs. total number of workers in the DNA system. • Information for the Supervisor these workers are connected to. • Time until next refresh

VIEWING WORKER INFORMATION FROM THE WORKER MACHINE

You can track DNA Worker statistics on each worker machine. A graphic-based interface is available on DNA worker workstations.

ACCESSING THE DNA WORKER INTERFACE ON A WINDOWS SYSTEM

Access the DNA Worker interface by clicking the DNA Worker icon on the Worker computer in the Windows system tray .

ACCESSING THE DNA WORKER ON A MACINTOSH, LINUX, OR PS3 MACHINE

To access the java-based DNA Worker interface on a Macintosh, Linux, or PS3 machine, complete the following:

1. At the command line of the machine, go to the /opt/Accessdata DNA3/Worker directory.

Type ./dna3workerd status

UNDERSTANDING THE DNA WORKER INTERFACE

The new DNA Worker interface runs as a Java app, so it is the same on Windows, Linux, PS3, or Macintosh workstations. The following figure shows the new DNA Worker interface:

Figure 4-4 DNA Worker Information Screen

DNA Worker Information
Worker Information
Elapsed Idle Time : 18:47:27
Connected : Yes
Name/IP - Supervisor : dev-joyce2/127.0.0.1
Name/IP - Worker : dev-joyce2/10.2.2.66
Working Processors : 0
Idle Processors : 2
Processor Speed : 3000
Last Supervisor Contact Time : 01/28/09 10:40:41
Release Version : 3.04.00238
Job Information
Task Assigned - Worker Time : n/a
Expected Task Completion -Worker Time : n/a
# of Passwords in task : n/a
Passwords / Second : n/a
Job Name : n/a
Restart
About
Close

If you have performed a stealth installation of the worker, you will not see the Worker icon in the Windows System Tray. You can access the DNA Worker interface by double-clicking Worker.exe in the [*drive*]:\Program Files\AccessData\DNA 3\Worker directory.

The following table describes each component of the DNA Worker interface:

TABLE 4-2 DNA Worker Information Components

Component	Description
Worker Information	
Elapsed Idle Time	Idle time in HH:MM:SS since this worker was last active.
Connected	Yes or No, depending on whether this DNA Worker is connected to a supervisor.
Name/IP - Supervisor	Network name/IP address of the connected supervisor
Name/IP - Worker	Network name/IP address of this worker

TABLE 4-2 DNA Worker Information Components

Component	Description
Working Processors	The number of physical processors on the DNA Worker machine that are currently working on DNA jobs.
Idle Processors	The number of physical processors on the DNA Worker machine that are *not* currently working on DNA jobs.
Processor Speed	Speed of the processor on the motherboard of this machine.
Last Supervisor Contact Time	MM/DD/YY HH:MM:SS of last contact with the Supervisor.
Release Version	DNA installed release version information.
Job Information	
Task Assigned - Worker Time	HH:MM:SS Time spent so far on the assigned job or task.
Expected Task Completion - Worker Time	HH:MM:SS Estimated time remaining to allow the worker to complete the current task.
# of Passwords in task	Number of passwords found for this job or task. This number increments as passwords are found.
Passwords / Second	Current average passwords being tested per second.
Job Name	Job name of current file being processed.

MANAGING WORKERS AND GROUPS

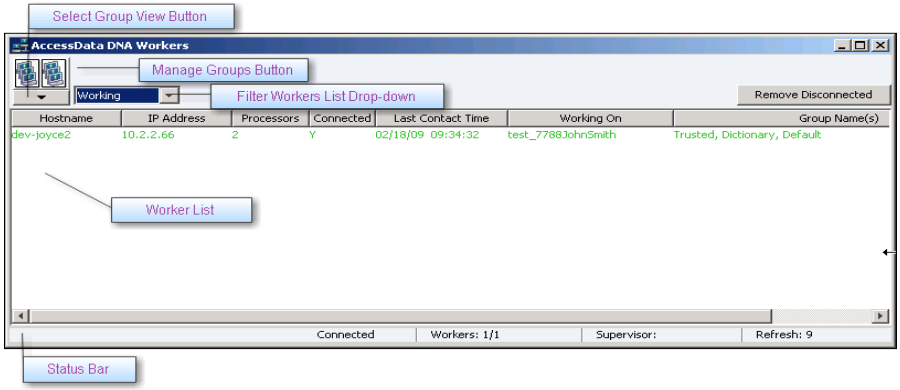
Managing Workers in a DNA System is done, in part, by creating Groups. Some tasks must be managed at the Group level; others can be managed at the Worker level.

FILTERING THE WORKERS LIST

The Workers List shows workers in a DNA system. You can filter the Workers List to show only the machines within a certain subnet, or only those workers that belong to a certain group.

To access the Workers Information dialogs, click *View* > *Workers Information*. To access the Workers List, click *View* > *Workers Information*.

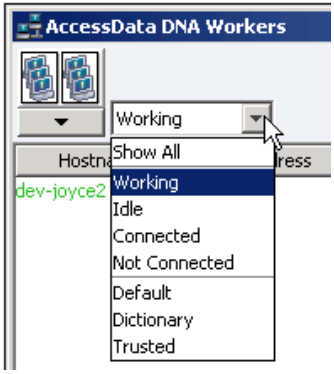
Figure 4-5 Viewing Workers Information



As you can see from the following figure, the Groups can be filtered by status: Working, Idle, Connected, and Not Connected.

The Groups can also be filtered by name: Default, Dictionary, and Trusted are the default groups. You can create new groups to meet your needs.

Figure 4-6 Selecting a Worker Filter



You can update the Workers List on the Filter section of the Edit Groups form. The following table describes the Filter form:

TABLE 4-3 Apply Filter Options

Component	Description
Field	A drop-down list that contains the following columns to sort by: • Name: The computer name of the worker. • IP Address: IP address of the worker. • Processors: The total number of physical processors on the supervisor or worker machine.
Expression	Enter any regular expression, including the following: • Period (.) to match any character. • Asterisk (*) to repeat the last character. • Plus Sign (+) to repeat the previous character. • [x–y] to signify the OR operation, and to specify a range of letters.
Access	A drop-down list of Allow or Deny that corresponds to the entry in the Expression field.

To filter the Workers List:

1. In the DNA Workers View, click *Filter*.
2. Select the Filter to use.
3. Click *Apply*. The Worker List is updated according to the filter specifications contained in that group's definition.

To clear the filter, click *Clear*. The current filter will be cleared, but not removed from the list.

MONITORING A DNA WORKER

You can view detailed statistical and graphical analyses of the performance of each DNA worker.

To view the worker status:

1. Select the workers in the Workers List.
2. Right-click the selection and choose *Properties*.

The Properties screen contains three windows organized as tabs, each with a particular focus or function. The tabs are labeled Information, Passwords/Second, and Availability. Each tab is discussed in the following sections.

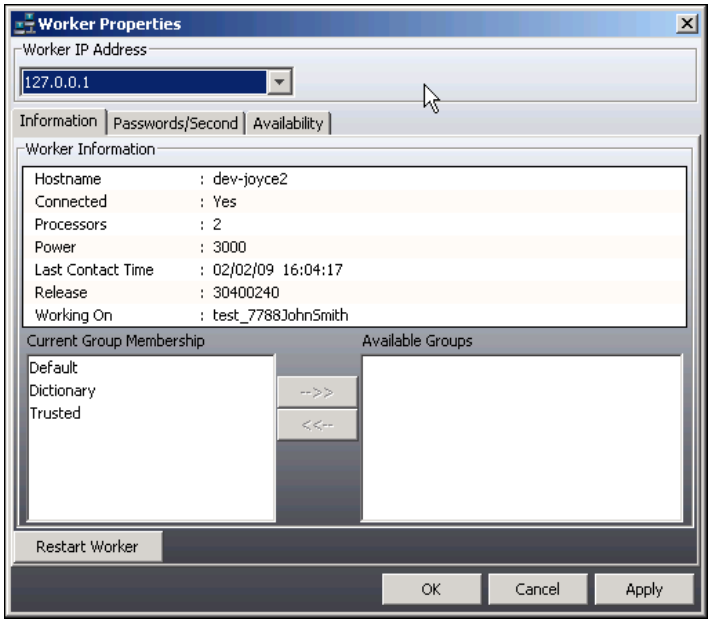
Note: You can resize the Worker Properties screen if desired.

To close the Properties screen, click *OK* or *Cancel*.

WORKER INFORMATION TAB

The Information window displays worker information, as shown in the following figure:

Figure 4-7 Worker Properties



The window is divided into one category about the worker and one category about the groups that the worker belongs to. Each category is discussed in the following sections.

WORKER INFORMATION

The following table describes the Basic Information section:

TABLE 4-4 Basic Worker Information

Item	Description
Hostname	The worker's network name.
Connected	Yes or No, depending on whether the worker is connected to the supervisor.
Processors	The number of internal processors this worker has
Power	
Last Contact Time	The last date and time this worker had contact with the Supervisor
Release	The program release and build of the DNA worker software.
Working On	The filename of the job currently being processed.

GROUP INFORMATION

The following table describes the Group Information section:

TABLE 4-5 Available Group Information

Item	Description
Processors	The total number of physical processors on the worker machine.
Power	The processor speed of the machine's physical processors. The program will average the processing speed of multiple processors selected.
Last Contact Time	The last date and time the supervisor contacted the worker.
Release	The version of the DNA that the machine is running.
Working On	The job name and attack type that the worker is processing. This field might be blank if the worker is not currently processing a job.
Group List	Names of groups that the worker belongs to.
Change Group Membership	Opens the Change Group Membership form so that you can quickly add or remove the worker from the listed groups. For more information about this form, see "Changing the Group Membership of a DNA Worker" on page 118.
Restart	Prompts to either restart the supervisor or worker or cancel restarting. You might restart the resource to update its group membership in the DNA management interface.

TABLE 4-5 Available Group Information

Item	Description
Item	Description
Processors	The total number of physical processors on the worker machine.
Power	The processor speed of the machine's physical processors. The program will average the processing speed of multiple processors selected.
Last Contact Time	The last date and time the supervisor contacted the worker.

AVAILABLE GROUPS

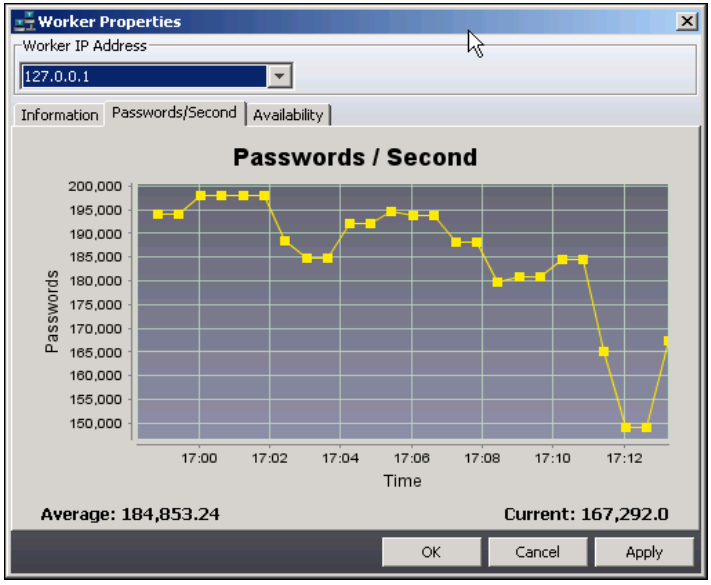
The Available Groups pane lists groups that this worker is not currently a member of.

PASSWORDS/SECOND TAB

The Passwords/Second window displays a graph of the number of passwords per second that are tested for validity over a given amount of time on the selected worker.

The following figure shows the Passwords per Second tab:

Figure 4-8 Worker Properties Passwords per Second



When viewing the properties of an individual worker, then this graph displays the passwords per second of the worker for the specified interval. The bottom of the

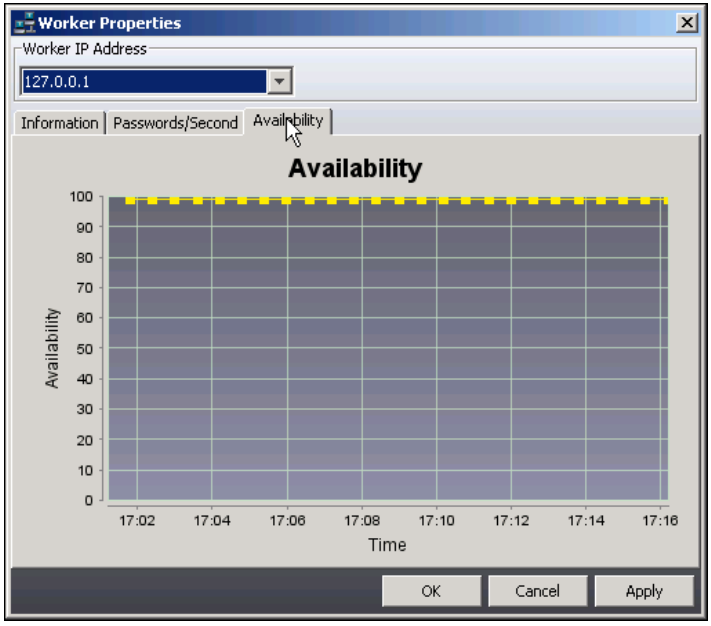
window displays the average number of passwords per second for the selected time interval.

Password statistics can be misleading because some types of encryption, such as Pretty Good Privacy (PGP), take more effort to test passwords on than other types of encryption, such as a Zip file. Also, the same encryption type can contain options that take longer to test. For example, one machine performing 1,000 password tests per second on a PGP disk file is working much harder (or much faster) than another machine performing 1,000,000 password tests per second on a Zip file.

AVAILABILITY

The Availability window displays a graph of the time when the worker is available. The following figure shows the Availability tab:

Figure 4-9 Worker Properties Availability



The Availability axis simply depicts if the resource is available or not; the range of numbers along the axis is purely for computational purposes. The bottom of the window displays the approximate availability for the selected time interval. The Availability statistics are useful metrics in understanding when the worker is most or least available to process jobs. Availability is not configurable.

CREATING A GROUP

You can create a group to manage DNA workers. For example, if a DNA supervisor manages 30 worker machines, you might create three groups of ten workers, each based on location or processing power. If you have a job that requires a quicker decryption rate, you can assign it to the most powerful group.

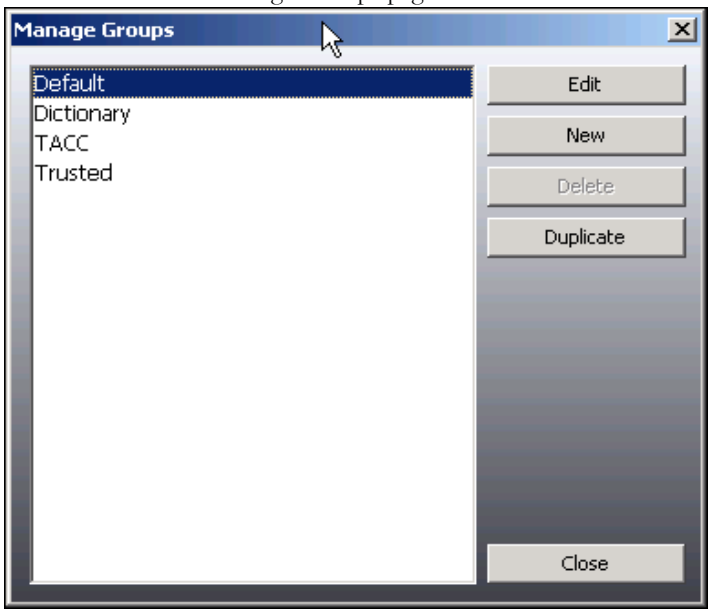
By default, DNA creates three groups:

- **Default**: Use to process the majority of files. All workers are assigned to this group.
- **Trusted**: Use to process ZIP, ARJ, RAR, PGP, Invisible Secrets, and EMF files. You must assign workers to the Trusted group before DNA can process jobs with the group. For more information, see "Changing the Group Membership of a DNA Worker" on page 118.
- **Dictionary**: Use to process files that only require a dictionary attack.

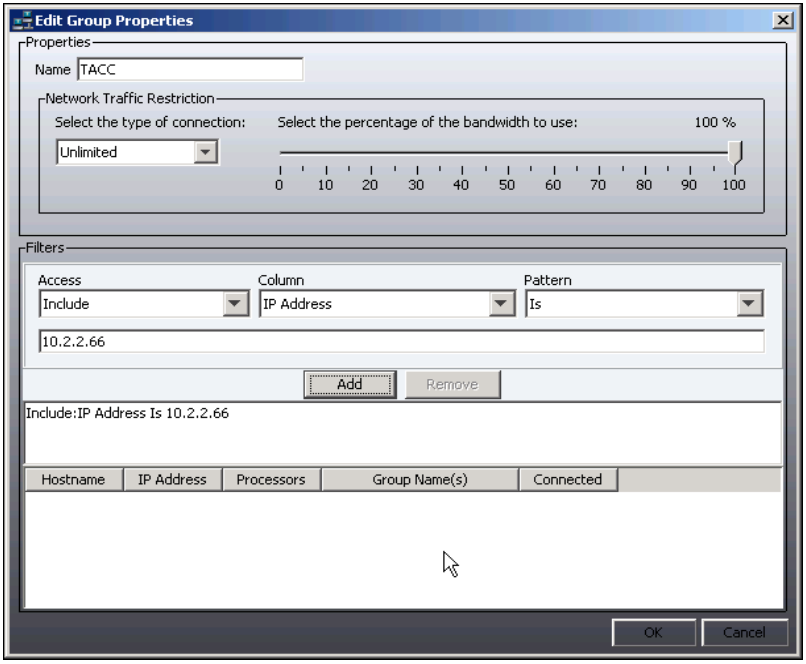
You use the Manage Groups form to create a group. To create a group:

1. Click the Manage Groups button in the AccessData DNA Workers View.

2. Click *New* on the Manage Groups page.



3. In the **Group Name** field, enter the name of the group and click *OK*. You might enter a name based on the location or power of the workers.



4. After you create a group, you can then assign workers to the group using the Filters feature.

EDITING A GROUP

You can edit an existing group to better suit your needs.

To edit a group:

1. Click *Manage Groups* in the AccessData DNA Workers View.

2. Select the group that you want to edit from the Manage Groups list and click *Edit*.
   - To change the group name, enter the new group name in the field.
   - To specify the speed at which DNA downloads dictionaries to the workers, select the type of network connection for the group and the percentage of connection bandwidth to use.

- To apply a filter to the group, click *Add* and complete the Filter section of the page.

3. After the changes are complete, click *OK*.

You can manage the Groups to help manage the Workers List. The following table describes the Edit Group Properties dialog:

TABLE 4-6 Edit Group Properties

Component	Description
Properties	
Name	The name of the group being edited
Network Traffic Restriction	Restricts a group to use only certain network types. Options include: • Unlimited • OC12 • OC3 • OC1 • T4 • T3 • T2 • T1 • DSL • 2 ISDN B Channels • ISDN B Channel • 56k Line • 33.6 Modem • 28.8 Modem • 14.4 Modem
Bandwidth Percentage	This is a sliding scale from 0 to 100% of available bandwidth that this group is allowed to use.
Filters	
Access	Access to the Supervisor. Options are: • Include • Exclude
Column	A drop-down list that contains the following columns to sort by: **Name**: The computer name of the worker. **IP Address**: IP address of the worker. **Processors**: The total number of physical processors on the supervisor or worker machine. **Group Name(s)**
Pattern	The pattern to follow, narrowing or broadening the workers to include in this group. Options are:

TABLE 4-6 Edit Group Properties

Component	Description
	• Is • Ends With • Begins With • Contains Once you have made your filter selections in the long text box below the Access, Column, and Pattern boxes, type the corresponding data that matches your Pattern selection, then click *Add*. In the Workers List below the filters you have set, you will begin to see the workers that match the filter display. You can do this for the Default, Dictionary, and Trusted groups, and for any custom groups you create.

DELETING A GROUP

It is possible that a group you have created in the past may outlive its usefulness. You can delete such a group easily.

To delete a group:

1. In the Workers List, click *Manage Groups*.
2. In the Manage Groups list, select the group that you want to delete and click *Delete*.
3. Click *Close*.

   Note: You cannot delete any of the three default groups. You can only delete custom groups.

CHANGING THE GROUP MEMBERSHIP OF A DNA WORKER

After you create a group, you can then assign workers to the group. You might assign a worker to become a member of a group because you need the machine's processing power in a group. A worker can be a member of more than one group. A powerful machine can be part of several groups to help process jobs more quickly.

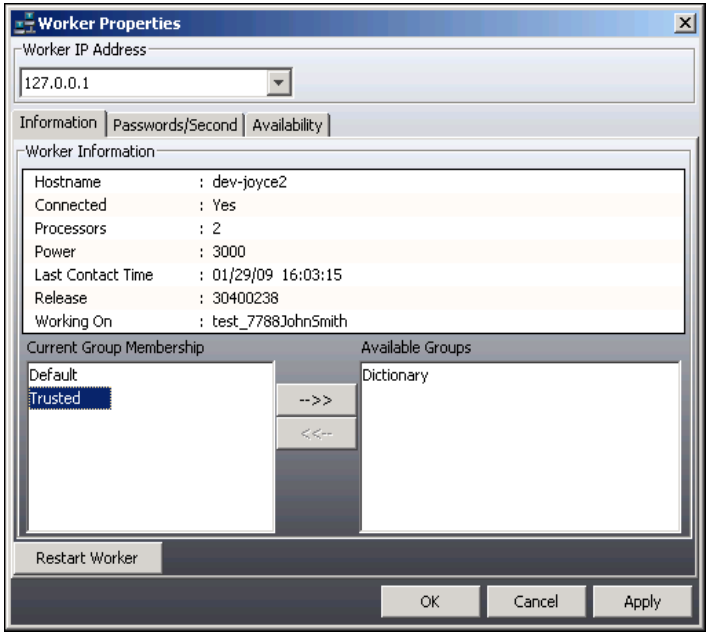
If you want to use the default Trusted group for sensitive files, you need to first assign workers to the group. You can change group membership on the Change Group Membership form.

To assign group membership to a worker:

1. Click *View* > *Workers Information*.

2. In the Workers List, right-click the worker you want to assign or change the Group Membership for and click *Properties*.
3. If the desired group is not already listed in the Current Group Membership list on the left, select the group to assign from the Available Groups list on the right, and click the double-arrow button to move it to the Current Group Membership list on the left.
4. Click *OK* to save the changes and to close the Worker Properties box.

Figure 4-10 DNA Workers: Change Group



To remove the worker from a group:

1. In the Current Group Membership list, select the group you want to remove the worker from.
2. Click the right-arrow button to move the unwanted group to the Available Groups list.
3. Click OK to save the changes and to close the dialog.

CHANGING THE SUPERVISOR OF A DNA WORKER

Change the supervisor assignment for a particular worker if you install a newer supervisor, or if you have multiple DNA systems:.

To change the supervisor of a DNA Worker:

1. In the worker list, right-click the worker you want to re-assign and click Change Supervisor.

Figure 4-11 Changing the Supervisor of a DNA Worker

2. Enter the IP address of the new Supervisor, or select it from the drop-down list.
3. Click OK to save changes and close the dialog, or click Cancel to abandon changes and close the dialog.

Chapter 5 Recovering Passwords

PRTK 6.5 and DNA 3.5 let you add files to recover passwords, monitor recovery jobs, view recovery results, verify hashes, and print recovery reports.

RECOVERY PROCESS OVERVIEW

You can add files to be recovered by selecting files using program options, or by dragging and dropping files into either the Job List Pane or into the DropFolder if you have one defined.

For every file you add to PRTK, at least one "job" is created. For each job, PRTK and DNA analyze the file to identify which modules to use and the attack types to perform, and to verify the possibility that the files can be decrypted or the passwords can be recovered.

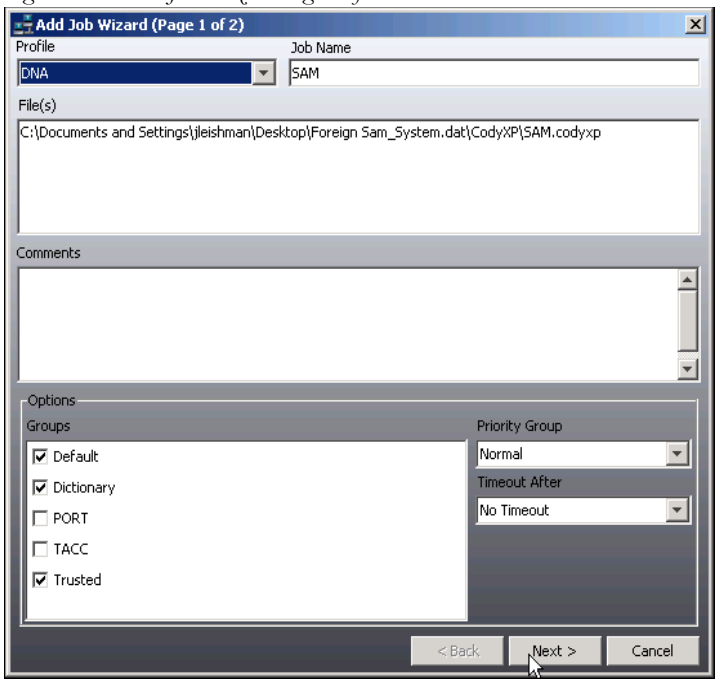
For certain files, a Module Options dialog displays the options you can select to define the attack options and recovery settings to use based on the type of file, its version, and the attacks available to be performed on the file. You can unmark the attacks you don't want performed on each file. For each attack type, a job is created. Thus, a single file can cause multiple jobs to be created.

Note: Some password recoveries are specialized and require additional steps. See "Chapter 9 Specialized Password Recoveries" on page 129.

Each job must be associated with a profile, which will be used during the recovery process. A profile defines details such as the dictionaries and rules to be used in the recovery process.

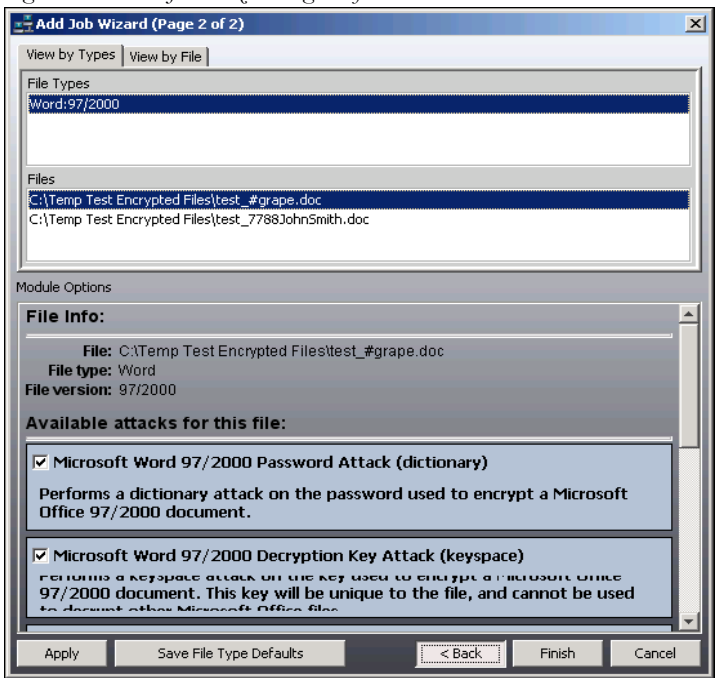
You can associate your job with the default profile, another included profile, or you can create your own customized profile. For more information, see “Setting a Default Profile” on page 96

Figure 5-1 Add Job Wizard Page 1 of 2



After you select a profile, if more than one attack type is available, you are prompted to verify which attack types to run.

Figure 5-2 Add Job Wizard Page 2 of 2


Add Job Wizard (Page 2 of 2)
View by Types
View by File
File Types
Word:97/2000
Files
C:\Temp Test Encrypted Files\test_#grape.doc
C:\Temp Test Encrypted Files\test_7788JohnSmith.doc
Module Options
File Info:
File: C:\Temp Test Encrypted Files\test_#grape.doc
File type: Word
File version: 97/2000
Available attacks for this file:
Microsoft Word 97/2000 Password Attack (dictionary)
Performs a dictionary attack on the password used to encrypt a Microsoft Office 97/2000 document.
Microsoft Word 97/2000 Decryption Key Attack (keyspace)
97/2000 document. This key will be unique to the file, and cannot be used
Apply
Save File Type Defaults
< Back
Finish
Cancel

PRTK or DNA generates the Rules and the necessary attack type(s), adds the job(s) to the list of jobs in the Job Queue Pane, and displays the job(s) in the View All tab.

PRTK or DNA then creates hash values for the files and performs the recovery process on the added jobs, which you can pause and resume. You can stop a job by deleting it.

Note: After you start a job, do not move the original files from the original location they were added from, until after the related job(s) complete.

While jobs are being processed, you can continue to add files. If you have defined a DropFolder, the files added there do not affect the jobs added manually.

BEST PRACTICES FOR ADDING JOBS

To maintain system performance, AccessData recommends the following:

- Do not add more than 50 files at one time.

- If a desired file on a network is larger than 10 MB, copy the file to the supervisor machine and then add it locally. While a removable drive is considered "local", the connection to that drive may cause a bottleneck and slow processing.
- Do not run a job on network drives or folders. Processing files across the network generates a large amount of network traffic.

ADDING JOBS

You can add files to be recovered by selecting files, or by dragging and dropping files into either the Job Queue Pane or into the DropFolder if you have one defined.

When you add a job, the job must be associated with a profile. The original source application doesn't have to be installed on the machine in order for DNA to process the job.

By default, PRTK and DNA include several profiles, some are exclusively for English files. You can associate your job with the default profile, or you can create your own profile that is more specific to the file that you are working with. For more information, see "Creating a Profile" on page 72.

SELECTING FILES

You can add files to be recovered by selecting files.

To select files for a recovery job:

1. From the menu bar, select *File* > *Add Files*.

   OR

   Click the *Add Files* button .
2. Browse to and select the file or files you want to add as job(s).

   Press *Shift+click* to select multiple contiguous files. Press *Ctrl+click* to select multiple discontiguous files.
3. Click *Add*.

   PRTK or DNA analyzes the file type and determines which attack types can be performed.
4. In the Add Job Wizard (Page 1 of 2), select the profile to use on these files for this password recovery job; then click *Next*.
5. (Conditional) In the Add Job Wizard (Page 2 of 2) dialog, select or unselect the module options you want for each file; then click *Finish*.

Note: If this has not been done in the past for the specific file type being added, the dialog will come up. If this has been done and the *Select File Type Defaults* button has been marked for this particular file type, you may not see this option dialog.

PRTK or DNA generates the recovery process settings for the job and displays an error only if the file could not be added.

DRAGGING AND DROPPING FILES

You can add files to be recovered by dragging and dropping files into the Job Queue Pane of either PRTK or DNA.

Important: This feature currently does not work in Vista. You can still add jobs by selecting files, as detailed in the above section.

To drag and drop files into PRTK or DNA:

1. In Windows Explorer, select the file(s) you want to add as a job.

   Press *Shift+click* to select multiple contiguous files. Press *Ctrl+click* to select multiple non-contiguous files.

2. Drag and drop the selected file or files into the Job Queue Pane.

   PRTK or DNA analyzes the file type and determines which attack types can be performed.

3. In the Add Job Wizard (Page 1 of 2), select the profile to use on these files for this password recovery job; then click *Next*.

4. (Conditional) In the Add Job Wizard (Page 2 of 2) dialog, select or unselect the module options you want for each file; then click *Finish*.

   Note: If this has not been done in the past for the specific file type being added, the dialog will come up. If this has been done and the *Select File Type Defaults* button has been marked for this file type, you may not see this option dialog.

5. PRTK or DNA generates the recovery process settings for the job and displays an error only if the file could not be added.

MONITORING JOBS

After you add a job to the job queue, you can monitor the job in several ways, including monitoring the password attacks or looking at statistics and graphical analyses of that job.

MANAGING THE RECOVERY PROCESS

PRTK lets you manage the recovery process of the jobs in the recovery session. This section reviews the tools you can use to manage the recovery session:

STOPPING AND STARTING THE RECOVERY SESSION

You can stop or start the recovery session by exiting or opening PRTK. DNA runs the services differently than PRTK, so exiting the DNA Supervisor does not stop the jobs from running.

To close the session, select *File* > *Exit*.

When you run PRTK again, the recovery jobs in the session appear in the PRTK window.

Note: When recovering passwords, PRTK independently analyzes and tracks the progress of each file. Consequently, you can close a session before all of the password recoveries are completed and then open the session later to have PRTK resume the password recoveries where it left off.

PAUSING JOB PROCESSING

You can pause recovery processes for all jobs in the recovery session or for selected jobs only.

To pause recoveries for all jobs, click *File* > *Pause All*.

To pause recoveries for selected jobs:

1. Select the job(s) to pause.
2. Right-click on the selected job(s).
3. Click *Pause*.

RESUMING JOB PROCESSING

You can resume recovery processes for all paused jobs in the recovery session or for selected jobs only.

To resume recoveries for all jobs, click *File* > *Resume All*.

To resume recoveries for selected jobs:

1. Select the job(s) to resume.

2. Right-click the selected job(s)
3. Click *Resume*.

REMOVING JOBS

You can remove all jobs in the recovery session or selected jobs only.

To stop processing and remove all jobs, click *File* > *Delete All*.

To stop processing and remove selected jobs:

1. Select the job(s) you want to remove.
2. Right-click the selected job(s).
3. Click *Delete*.

SPECIFYING RECOVERY PREFERENCES

You can set default recovery settings to use when processing jobs in the recovery session. These options are covered in-depth in Chapter 3. For more information about setting preferences, see "Changing Preferences" on page 39.

DISPLAYING JOB PROPERTIES

You can view detailed statistical and graphical analysis of the jobs in the recovery session.

View the properties of a job by doing any one of the following:

- Double-click a job.
- Right-click a job and select *File Properties*.
- Select a job and click *View* > *File Properties*.

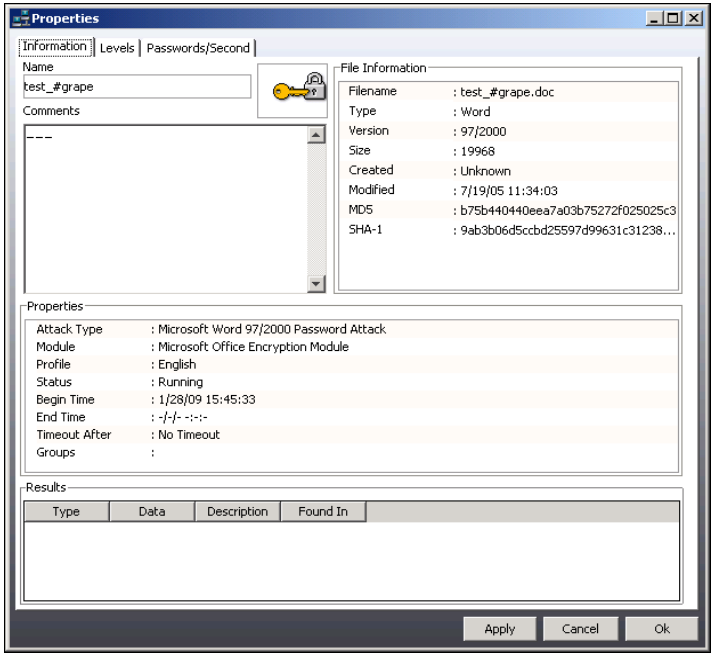
The Job Properties screen contains three windows organized as tabs, each with a particular focus or function. Each tab is discussed in the following sections. You can resize the Job Properties screen if desired.

To close the Job Properties screen, click *OK* or *Cancel*.

JOB INFORMATION TAB

The Information window displays basic job information and the results of the job processing.

Figure 5-3 Viewing Job Information



The window is divided into four categories. Each category is discussed in the following sections.

BASIC INFORMATION

The following table describes the Basic Information section:

TABLE 5-1 Basic Job Information

Item	Description
Name	The job name. Once created and added, this cannot be changed.
Comments	Any comments you entered in the Add Job Wizard, or any commands from the Job Properties screen. You can also add comments here while the job is running.

FILE INFORMATION

The following table describes the File Information section

TABLE 5-2 Job File Information

Item	Description
Filename	Filename of the job.
Type	Application that the file was created in.
Version	Version of the file format recognized by PRTK modules.
Size	Size of the file in bytes.
Created	Date and time that the file was originally created, if available.
Modified	Date and time that the file was last modified.
MD5	MD5 (128-bit) hash of the file data.
SHA-1	SHA (160-bit) hash of the file data.

PROPERTIES

The following table describes the Properties section on the Job Information Tab:

TABLE 5-3 Job Properties Information

Item	Description
Attack Type	Attack type used for this particular instance of the job.
Module	Recovery module used for the attack. The module is based on the combination of file type and the attack type.
Profile	The profile assigned to the job using the Add Job Wizard.

TABLE 5-3 Job Properties Information

Item	Description
Status	The status of the job. The following are the possible states: • **Depends On**: The job is dependent upon the completion and results of another job before it can start its processing. • **Finished No Passwords Found**: The job is completed and no passwords were found. • **Finished** *password*: The job is completed and the password is displayed. If the password contains a space, <space> displays in the appropriate location, for example, AccessData<space>Corporation. • **Paused**: The job is paused. • **Queued**: The job is not yet assigned for processing. • **Running**: The job is being processed. • **Waiting**: The job is dependent upon the completion of, or timeout of, another job before it can start its processing.
Begin Time	The date and time that processing began.
End Time	The date and time that processing finished.
Timeout	How long PRTK or DNA performs the dictionary attack before it times out and begins a different attack. This is set in the Add Job Wizard, Page 1 of 2, under Timeout. **Note:** For very large jobs, it may be best to set the Timeout to No Timeout. Otherwise, it can timeout before the job even gets added.
Groups	The groups to which the job is assigned. Default group names are: • Default • Dictionary • Trusted You can create custom groups according to your needs, or to accommodate add-ons such as a Tableau* TACC* unit, or AccessData PORT or Hash Tables.

RESULTS

The Results section displays the passwords and keys that PRTK discovers during the decryption process.

The Results section might have multiple entries even if a password is discovered in the first entry. Some files, such as Adobe* PDF documents and Word documents, can have

multiple passwords. Even though one password is discovered, more tests might still be running on lower priority Rules.

The following table describes the Results section.

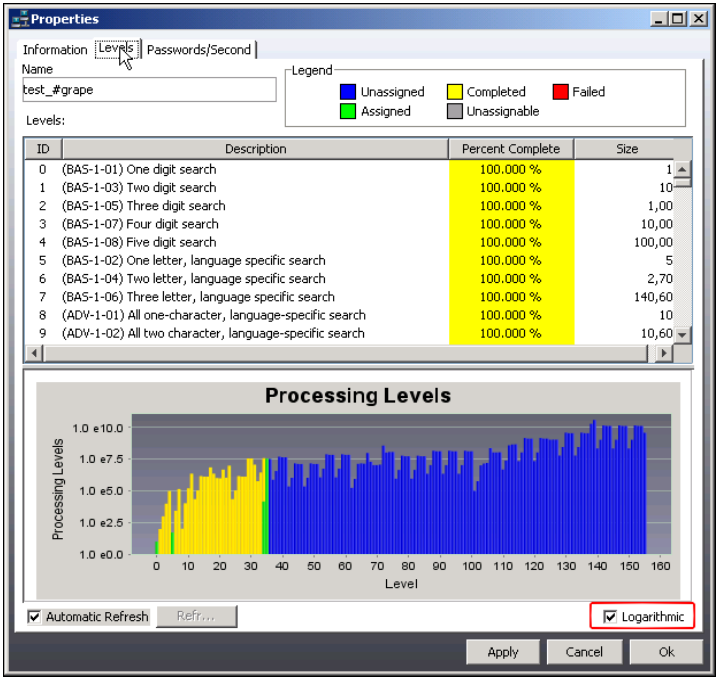
TABLE 5-4 Job Results Information

Column	Description
Type	Either password or key, depending upon what is decrypted first.
Data	The actual password or key that decrypts the file.
Description	The type of password or key that is found. The type is defined by the specific application that the file was encrypted in. The following are possible types: File, User, Owner, Administrator, Assistant, Reader, Definer, Supervisor, Spare, Possible, Read-Write, Service Website, Field, Write Reservation, Option Protect, Sheet, Save As, Title, Protection, Transaction, Data Entry, Payroll, Spare User, Pass Key, and Zip Key.
Found In	The Rule and corresponding dictionary that the password or key was discovered in.

JOB RULES TAB

The Rules tab displays information about the recovery Rules specified in the profile that was selected for that job. It also displays a graph that illustrates the number of decryption attempts per recovery Rule and the progress of the attack

Figure 5-4 Job Properties Job Rules Tab with Logarithmic Display



You can zoom in on the graph to display a greater level of detail. Click the desired region and drag the mouse to create a rectangle that covers the area you want to see.

The following table describes the information displayed in the Rules tab:

TABLE 5-5 Job Rules Information

Component	Description
Name	The name of the job about which recovery Rule information is displayed.

TABLE 5-5 Job Rules Information

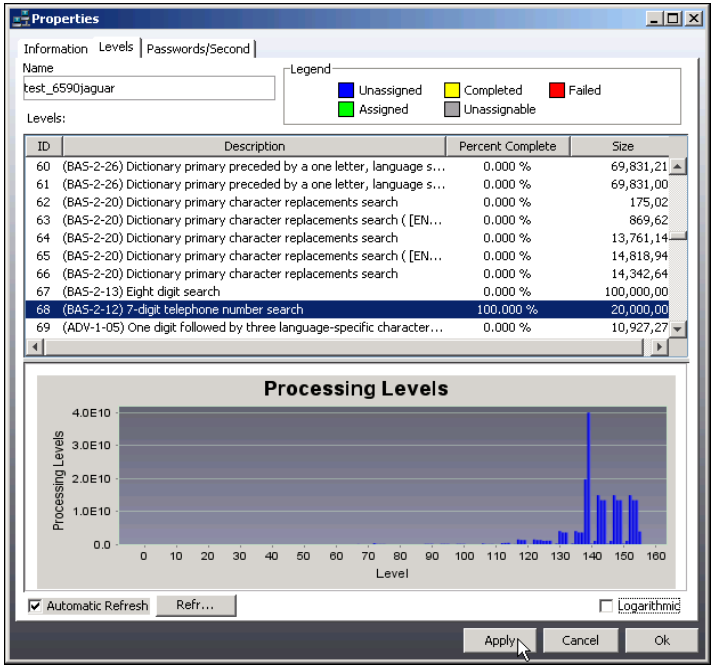
Component	Description
Legend	 A color key for the Rules displayed in the graph. The following list describes each Rule: • **Unassigned**: A Rule has not yet been assigned to that job. • **Assigned**: The Rule is assigned to be processed. • **Completed**: The Rule has completed processing. • **Unassignable**: The Rule has been allocated to another resource. • **Failed**: The Rule was assigned, but the program did not return the results.
Rules	Rules information related to the selected profile. The information categories are as follows: • **ID:** The ID number assigned to the Rule by PRTK or DNA • **Description:** The Rule and corresponding dictionary that the Rule is run on. If you do not want to process a Rule in the graph, right-click the Rule before it is assigned, and select *Skip*. A skipped Rule is not processed. **Note:** A skipped Rule is immediately marked as 100% complete. • **Percent Complete:** The percentage of password or key combinations that have been tried for that Rule. • **Size:** The total number of possible password or key combinations produced by that Rule.

The Rules tab graph can be displayed two different ways. By default, PRTK displays the graph with the *Logarithmic* box checked. The graph displays great detail about how many tries are attempted at each recovery Rule. The graph shows a relative view of the number of tries that are shown so that you can see each attempt in greater detail.

If you uncheck the *Logarithmic* box, then click *Apply*, a larger-scale graph displays that shows a more general view of the Rule progress. An example of this type of graph is shown below. The non-logarithmic graph displays the last few Rules much larger than

all the others. This type of graph displays the comparative relationships between the Rules more accurately.

Figure 5-5 Job Properties Job Rules Without Logarithmic Display



You can set the view on the Rules tab to refresh automatically, or to manually refresh.

To change the Refresh setting:

1. Mark the box labeled Automatic Refresh to have this screen update itself automatically.

   This setting deactivates the Refresh button.

   OR

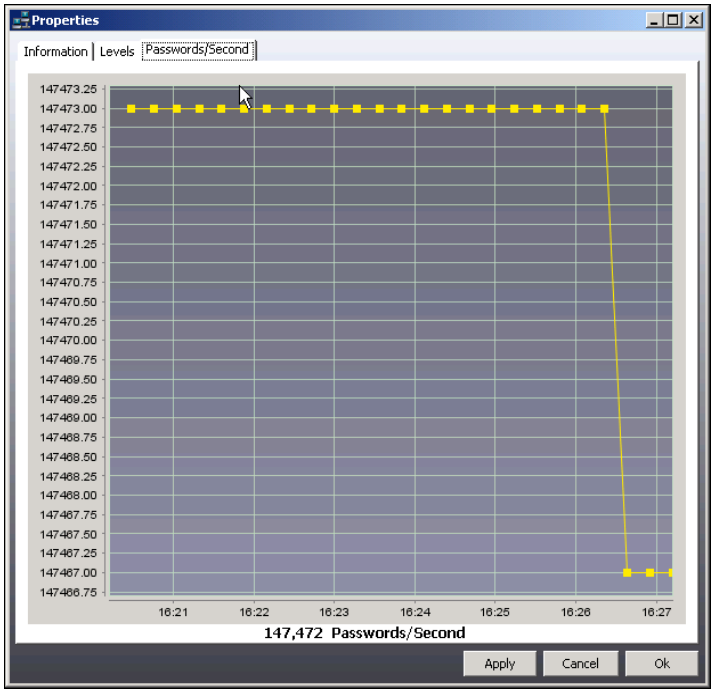
   Unmark the Automatic Refresh box to disable automatic refresh and activate the Refresh button. Click *Apply* to save your changes.
2. Click *OK* to close the entire Properties dialog.

PASSWORDS/SECOND

The Passwords/Second window displays a graph of the number of passwords per second that are tested for validity over a given amount of time on the selected job. The

bottom of the window displays the average number of passwords per second for the selected time interval

Figure 5-6 Job Properties Passwords/Second Display



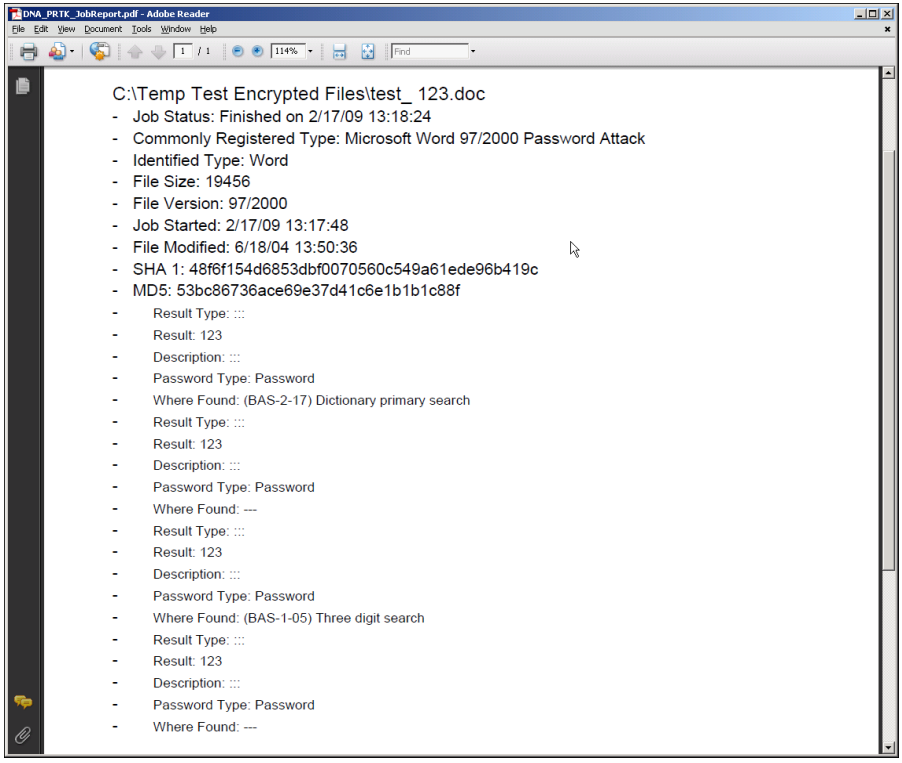
Password statistics can be misleading because some types of encryption, such as PGP, require more effort and time to test passwords than other types of encryption, such as a Zip file. Also, the same encryption type can contain options that take longer to test.

For example, one machine performing 1,000 password tests per second on a PGP disk file is working much harder (or much faster) than another machine performing 1,000,000 password tests per second on a Zip file.

PRINTING RECOVERY REPORTS

You can print reports containing file information for jobs in the Job Queue Pane. Job reports are generated in .PDF format.

Figure 5-7 Generated Recovery Report


DNA_PRTK_JobReport.pdf - Adobe Reader
File Edit View Document Tools Window Help
C:\Temp Test Encrypted Files\test_ 123.doc
- Job Status: Finished on 2/17/09 13:18:24
- Commonly Registered Type: Microsoft Word 97/2000 Password Attack
- Identified Type: Word
- File Size: 19456
- File Version: 97/2000
- Job Started: 2/17/09 13:17:48
- File Modified: 6/18/04 13:50:36
- SHA 1: 48f6f154d6853dbf0070560c549a61ede96b419c
- MD5: 53bc86736ace69e37d41c6e1b1b1c88f
- Result Type: :::
- Result: 123
- Description: :::
- Password Type: Password
- Where Found: (BAS-2-17) Dictionary primary search
- Result Type: :::
- Result: 123
- Description: :::
- Password Type: Password
- Where Found: ---
- Result Type: :::
- Result: 123
- Description: :::
- Password Type: Password
- Where Found: (BAS-1-05) Three digit search
- Result Type: :::
- Result: 123
- Description: :::
- Password Type: Password
- Where Found: ---

Reports contain file attributes information, including filename, registered type, identified type, size, file version, created, modified, and hash values (SHA and MD5). For information on attributes, see "Displaying Job Properties" on page 77.

To print a recovery report:

1. Select *File* > *Generate Report.*
2. Browse to the location for saving the report.
3. Give the report a name.
4. Click *Generate.*

MANAGING JOBS IN DNA

The following additional options and tasks are available for managing jobs in DNA that are not available in PRTK.

ALLOCATING RESOURCES FOR A JOB

You can allocate the percentage of DNA Workers in a supervisor group that works on a particular job. By default, DNA automatically divides the number of jobs between the available processors on all the machines in the supervisor group.

DETERMINING HOW WORKERS PROCESS JOBS

You can determine the amount of data sent to each worker so that the worker machines don't receive more than they can handle.

After the DNA Worker program is installed on a machine, DNA detects its processing power. DNA sends appropriate amounts of data based on the power of each machine. You can specify the chunk size for sending jobs to a worker.

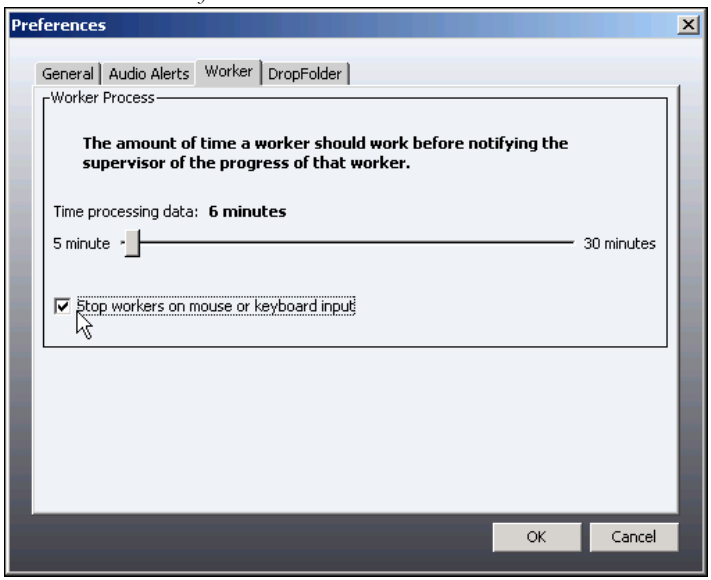
By default, DNA Workers always use a low-priority thread on the machine to process jobs. However, you can choose to have workers process jobs only when the machines are idle. DNA determines a machine is idle if the mouse and the keyboard aren't being used on the machine.

You can change the job processing setting for all workers in the DNA system or only for workers subordinate to a particular supervisor.

Note: You cannot change the job processing setting for DNA Workers running on Windows 98 or ME machines.

To specify when workers process jobs:

1. Select *Edit* > *Preferences.* > *Worker Tab*



Chunk size is the amount of the password set or keyspace the Supervisor sends to the Worker, anticipating what the Worker can process in the amount of time allotted.

To change the process duration,

2. Slide the bar right to increase the number of minutes, or left to decrease the number of minutes.
3. Click *OK*.

To change when the workers process jobs, check the *Stop Workers on Mouse or Keyboard Input* box. This suspends the processing of jobs by the worker while the human user is active on the computer. When mouse or keyboard activity stops and remains inactive for approximately ten minutes, the Worker will resume processing of jobs automatically.

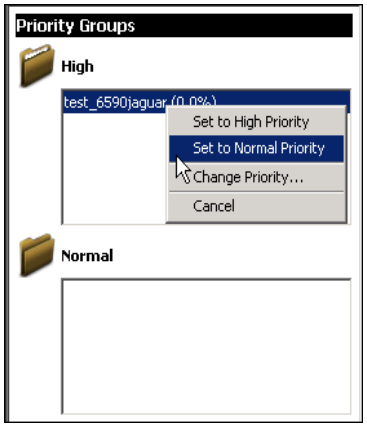
CHANGING THE PRIORITY GROUP OF A JOB

You can change the priority group assigned to a job. The priority group determines which jobs are processed with greater resources.

DNA has two priority groups: High and Normal. You might change the assigned priority group to High if you want the job to be processed more quickly. Or change the

priority group to Normal if you want to place a different job or jobs in High priority status. The following figure illustrates this:

Figure 5-8 Changing Priority Groups



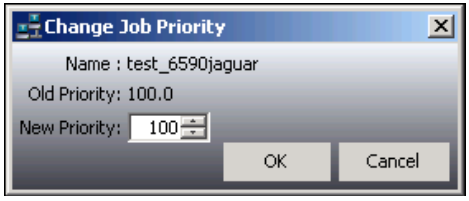
To change the priority group of a job:

1. In the Priority Groups list, select the job that you want to change.
2. Right-click and select *Priority Group*.
3. Choose *High* or *Normal*.

CHANGING THE PRIORITY OF A SINGLE JOB

You can change the priority of a single job on the Change Job Priority form. The job priority determines the percentage of available resources within a DNA Supervisor's control that can work on a particular job. This is illustrated in the following figure:

Figure 5-9 Changing Job Priority



To change the priority of a job:

1. In the Priority Groups pane, select the job that you want to change the priority of.
2. Right-click and select *Change Priority*.

3. In the New Priority field, click the up or down arrows until you reach the desired priority.

   OR

   Clear the current entry in the New Priority box, and type in the new priority number you want to assign for this job.

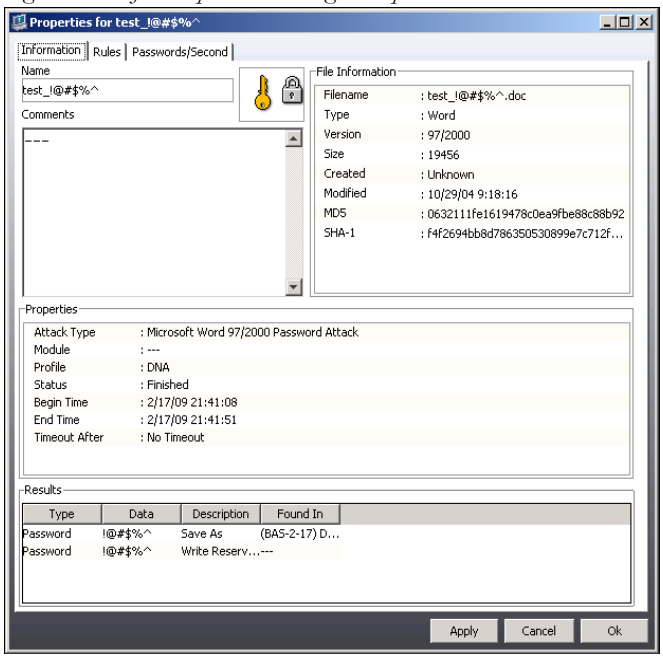
4. Click *OK*.

OPENING FILES USING RECOVERED PASSWORDS AND KEYS

MANUALLY DECRYPTING FILES WITH A PASSWORD OR KEY

After DNA discovers a password or key for an encrypted file, it displays the password or key in the Results section of the job Properties screen, shown below. You must then apply the password or key to decrypt the file.

Figure 5-10 Job Properties Showing Multiple Passwords



Saving Decrypted Files Manually

After PRTK recovers the decryption key of a file, you can manually decrypt and save the file.

To manually decrypt a file after recovering the key:

1. In the Job Queue pane, right-click a job that has a recovered decrypt key.
2. Select *Decrypt* from the menu.
3. Specify where to save the decrypted file.

Decrypting with a Key

You can choose to decrypt an encrypted file with a key on a file-by-file basis. You might decrypt a file individually because you want to closely manage the content of the decrypted file.

You can also choose to have DNA automatically decrypt the file after the key is discovered. For more information, see "Changing Preferences" on page 39.

Copying a Recovered Password to the Clipboard

After PRTK or DNA recovers a password, you can copy the password to the clipboard to use when opening the file in its original application, if it is installed on the recovery computer.

To copy a recovered password to the clipboard:

1. In the PRTK or DNA Job Queue pane, right-click a job that has a recovered password (listed in the Results column).
2. Select *Copy password to clipboard* from the menu.
3. Run the original application, and when prompted for the password, click in the password field and press Ctrl-v to paste the recovered password from the clipboard.

Opening a File with a Recovered Password

After PRTK or DNA recovers a password, you can open the file in its original application from within PRTK or DNA.

Note: To open a file, the application in which the file was created must be available. For example, to open an Excel file, you must have Microsoft Excel installed on the computer.

To open a file with a recovered password from within PRTK or DNA:

1. In the PRTK or DNA Job Queue pane, right-click a job that has a recovered password (listed in the Results column).
2. Select *Open with default Application* from the menu.
3. When prompted for a password, press Ctrl-v to paste the recovered password from the clipboard.

For an explanation of encrypted files, see "Understanding Encrypted Files" on page 217.

MULTIPLE, SPARE, AND INTERNATIONAL PASSWORDS

In some recoveries, PRTK and DNA recover multiple passwords, spare passwords, or passwords with international characters.

MULTIPLE PASSWORDS

In some recoveries, PRTK and DNA might recover multiple passwords. For example, for system files, PRTK or DNA might recover the access passwords for multiple users. For FTP program files, PRTK or DNA might recover the login passwords for multiple FTP sites. In some cases, a single file might have multiple passwords with different rights associated with them. For example, one password could open the document, and another might be required to the modify the document.

SPARE PASSWORDS

In some recoveries, PRTK might not recover the original password that was used to lock the file, but might recover a "spare." The spare password can consist of a string of numbers or a combination of alphanumeric characters.

For example, when performing a password recovery using the Paradox module, PRTK recovers a password that is a string of numbers. This string of numbers acts just like a spare key to your car or home; it unlocks the document even though it is not the original password.

To open a file that has a spare password, type the recovered password. If the recovered password does not unlock the file, please contact AccessData support.

INTERNATIONAL PASSWORDS

PRTK and DNA have been used successfully to recover passwords for documents created in other languages, including Arabic, French, German, Italian, and Spanish.

When recovering passwords containing Extended ASCII or Unicode characters, PRTK displays password characters using the Microsoft Sans Serif font. Before opening a file, you need to determine the Alt keystrokes to enter for the password when opening the file.

To recover a password that has international characters:

1. After recovering a password with international characters, open the Windows Character Map by clicking *Start* > *Programs* > *Accessories* > *System Tools* > *Character Map*.
2. Select the *Microsoft Sans Serif* font.

Important: Make sure you are using the correct font. PRTK and DNA use Microsoft Sans Serif, and not MS Sans Serif.

3. In the lower-right corner of the window, find the Alt- keystrokes necessary to enter the character code.
4. Open the file and, when prompted for the password, enter the Alt- keystrokes for the character code displayed in the Microsoft Sans Serif character set.

   Note: When entering Alt- keystrokes, make sure NUM LOCK is on. Hold down ALT; then, using the numeric keypad, type 0 (zero) followed by the character code number.

Chapter 6 Managing Profiles

Before a job can be processed in PRTK or DNA, it must be added to an existing profile. A profile is a collection of specific rules, dictionaries, and other settings that are pertinent to a category of encrypted files.

DEFAULT PROFILES

PRTK and DNA share the same profile names. The following details the default profiles installed with PRTK and DNA, and a description of each.

TABLE 6-1 Default Profiles

Profile Name	Description
English (default)	Begins by searching for simple passwords, followed by dictionary and permutated dictionary searches, and ends with complex searches for dictionary and computed passwords. All default English dictionaries and character sets are used.
Arabic	Begins by searching for simple passwords, followed by, dictionary and permutated dictionary searches, and ends with complex searches for dictionary and computed password. All default Arabic dictionaries and character sets are used.
European	Begins by searching for simple passwords, followed by dictionary and permutated dictionary searches, and ends with complex searches for dictionary and computed passwords. All default German, French, Italian and Spanish dictionaries and character sets are used.
Russian	Begins by searching for simple passwords, followed by, dictionary and permutated dictionary searches, and ends with complex searches for dictionary and computed password. All default Russian dictionaries and character sets are used.

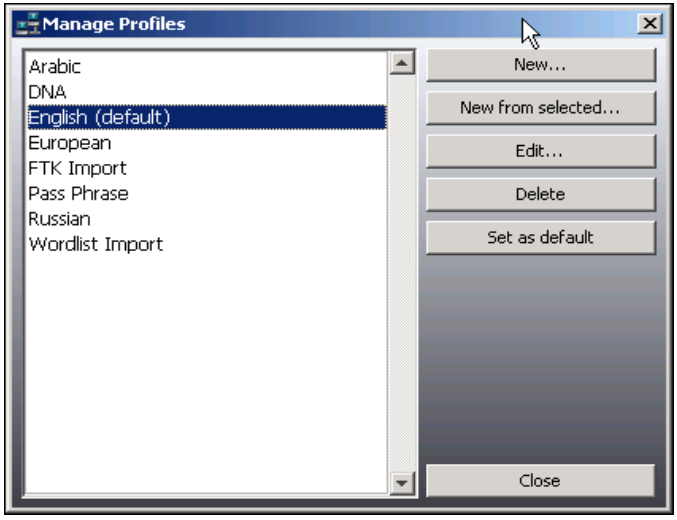
TABLE 6-1 Default Profiles

Profile Name	Description
Pass-phrase	Uses all pass-phrase Rules in English
FTK Import	Used as a template for FTK imported word lists
PRTK (PRTK only)	Rules in this profile are ordered by research conducted on recovered passwords. Each Rule completes in 24 hours or less based on a job processing 200,000 passwords per second.
DNA (DNA only)	Rules in this profile are ordered by research conducted on recovered passwords. Rules that can complete in five days or less are processed first, followed by Rules that take longer than five days to process (based on a job processing 200,000 passwords per second on one worker).

SETTING A DEFAULT PROFILE

You can set any profile as the default profile. Every job added to the PRTK system is assigned to the default profile unless you select a different profile for a job when it is added.

Figure 6-1 Managing Profiles



To set a default profile:

1. Select *Edit* > *Profiles*.

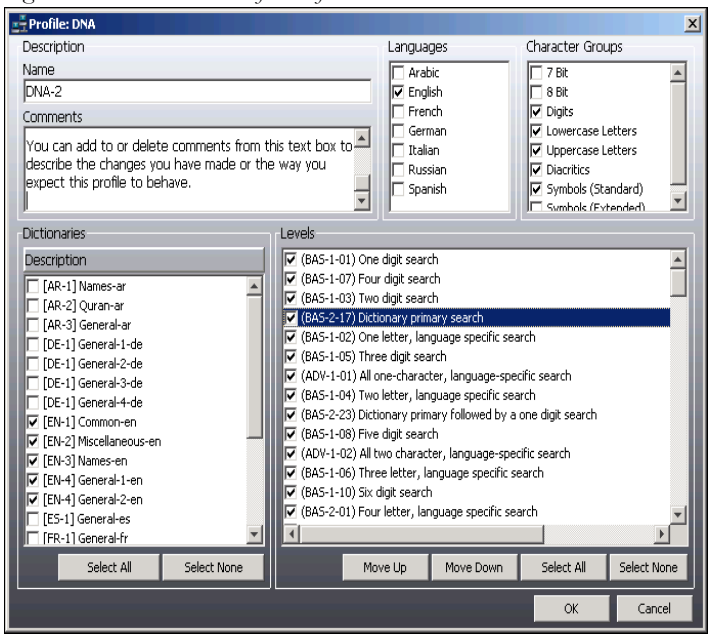
2. In the Manage Profiles list, select the profile that you want to set as the default, and then click *Set As Default*.

CREATING A PROFILE

You can create profiles specific to the files or cases with which you are working.

For example, if you have a collection of encrypted files from a case that has documents in both English and Arabic, then you can create a profile that includes only English and Arabic dictionaries. When PRTK or DNA processes the files, it only runs the selected rules on the selected dictionaries. This limiting process speeds up the decryption process for your files, and increases the likelihood of success.

Figure 6-2 The DNA Profile Definition Pane



You can use the New Profile pane to name the profile and select the languages, character groups, dictionaries, and rules to include in the profile. Some selections are made by default, but they can be changed. You must give the profile a name before clicking *OK*, or you will be prompted to do so.

The following table describes the Profile window:

TABLE 6-2 New Profile Options

Option	Description
Description	Information about the profile, including the name and any comments about the specific profile you are creating.
Languages	PRTK and DNA can process encrypted files in the following languages: • PArabic • English • French • German • Italian • Russian • Spanish
Character Groups	By default, Lowercase Letters, Uppercase Letters, Digits, Symbols, and Diacritics are checked. • The character selections do not affect the dictionaries. • Lowercase Letters: uses only lowercase letters to generate passwords. • Uppercase Letters: uses only uppercase letters to generate passwords. • Digits: Searches for numbers. • Symbols (Standard): Searches for symbols from the keyboard, such as the plus sign (+) or the dollar sign ($). • Symbols (Extended): Searches for symbols from the character tables, such as the Em dash (—) or the Yen (¥). • Diacritics: Searches for symbols, such as the tilde (~) or the circumflex (^) combines with letters. • All 7-bit Characters (ASCII): Searches for any ASCII characters. This box includes all characters listed above it. • All 8-bit Characters: Searches for any ASCII and Extended ASCII characters. This box includes all characters listed above it and the Extended ASCII characters.
Dictionaries	The following dictionaries are included in PRTK. Dictionaries end with the .ADF or .XML extensions. Each dictionary includes both a code page (-c.ADF) and a Unicode (-u.ADF) version. You can also create additional dictionaries from a forensic image. For example, you can create dictionaries from the word list from FTK.
Rules	The password Rules that PRTK applies to dictionaries. The Rules are run in the order you list.

To create a profile:

1. Select *Edit* > *Profiles* > *New* to create a new profile from a default template.

   OR

   Select *Edit* > *Profiles* > *New From Selected* to use a selected profile as a template.
2. In the Name field, enter the name of the profile. Without a profile name, the profile will not be saved.
3. In the Comments field, enter any comments that might be helpful to others working on the case, such as "Use this profile for files in Case 1."

   Note: It is recommended that you add comments to indicate the purpose of the profile, or some other useful or necessary information, whatever it may be. The contents of the Comments field can be edited at any time using the Profile Editor screen.
4. Check the languages to include.
5. Check the character groups to include.
6. Check the dictionaries to include.

   The dictionaries are checked by default according to the languages that you specify in Step 4. You can add more dictionaries that are relevant to your encrypted files.

   To aid in the selection process, click *Select All* or *Deselect All*.
7. Check the rules to include.

   To change the order of a rule, select the rule; then click *Move Up* or *Move Down*.

   To aid in the selection process, click *Select All* or *Deselect All*.
8. Click *Save* > *Yes*.
9. The *.profile file will be saved to the %systemroot%\documents and settings\all users\application data\accessdata\PR\Profles\ folder.

EDITING A PROFILE

You can edit any of the information that you originally specified when you created a profile. You might edit a profile if you want to change the order of the password rules or to add another dictionary that you have recently created. Edit a profile on the Manage Profiles screen.

To edit a profile:

1. Select *Edit* > *Profiles*.
2. In the Manage Profiles list, select the profile to edit and then click *Edit*.
3. Modify the desired options in the profile form.
4. Click *OK*, and then *Close*.

Note: You cannot change the name of the profile on this screen. If you enter a new profile name, then another profile with the same name as the profile that you are editing is added to the Manage Profiles list.

For more information about each option, see "Creating a Profile" on page 97.

DELETING A PROFILE

You may choose to delete a profile if you no longer need its specific collection of Rules and dictionaries. You can delete a profile on the Manage Profiles screen.

To delete a profile:

1. Select *Edit* > *Profiles*.
2. In the Manage Profiles list, select the profile that you want to delete and then click *Delete*.
3. Click *Yes* to confirm the deletion.

Chapter 7 Managing Password Recovery Rules

You can customize the password recovery rules that PRTK 6.5 and DNA 3.5 use in their file decryption. You can customize the rules either by creating a new rule or changing the rule order so that the time required to decrypt a file is decreased.

UNDERSTANDING RULE CATEGORIES

Rule ordering (the arrangement of rules when creating new profiles) started with rules of the fewest amounts of password tests and ended with rules of the greatest amount. Profiles are then created to reflect the rule order, with the idea that rules with the fewest tests (attempts) would complete first, in the least amount of time for each of the profiles created.

Several rules use the Markov permutation. These rules include words with phonemes that sound like English words; the words themselves, however, are actually meaningless.

If you select a rule that is language-specific and the profile contains a dictionary that cannot use the specific rule, PRTK and DNA simply do not generate any words from that rule. For example, if you have a profile that contains an Arabic dictionary and you select the Markov rule, PRTK does not apply the Markov rules to the Arabic dictionary because the Markov rules currently support only the English language.

Rules are ordered by a combination of the number of password tests and the types of password attacks. The label Basic (BAS), Advanced (ADV), or Pass-phrase (PP) is prefixed to the rule name according to the number and types of tests they perform. Some language-specific rules may fall into Basic Rules according to size, but are labeled as Advanced because of the choice of character groups that can be applied to a given

profile. Each rule has a prefix composed of a category, followed by an intensity, followed by an ID. For detailed information on rules, see "Rules" on page 196.

Default Rule Order

PRTK and DNA rules are arranged in a specific order by default. This order can be changed by the user. For a table listing the default rule order, see "Default Rule Order" on page 197.

Modifying the Password Rule Order

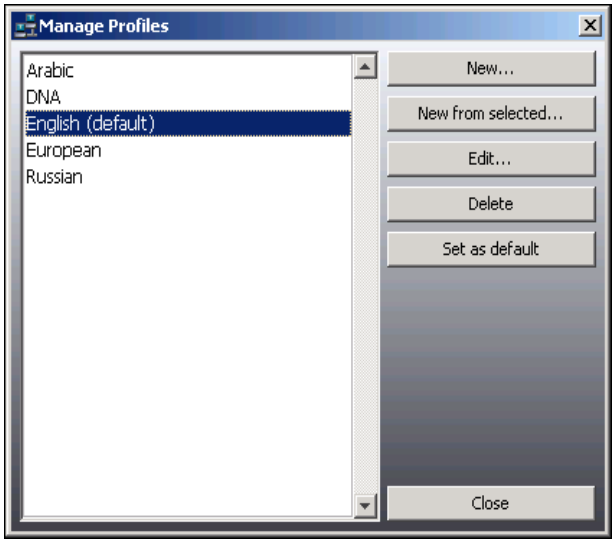
PRTK uses many different password rules to filter potential passwords through various permutations. The rules progress through the Golden Dictionary automatically, and subsequently all other selected dictionaries from the top of the list to the bottom. For a table that contains all password rules, see "Appendix B Password Recovery Attacks" on page 193.

You can change the order of the password rules to increase the speed of password recovery. For example, if you know the password is in English and contains three characters, you can move the "All Three-letter Language-specific Passwords Search" rule to the top of the Rules list.

You change the order of the password rules within a profile. You cannot automatically change the password rule order for all profiles.

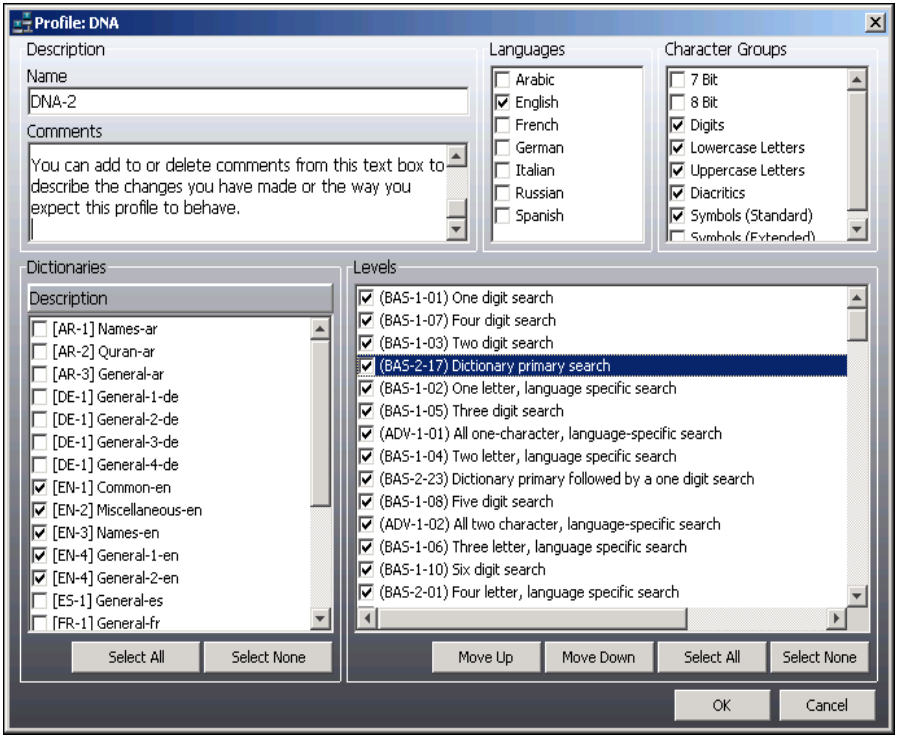
To change the password rule execution order for a profile:

1. Select *Edit* > *Profiles*.



2. Select the profile that you want to change, then click either *New*, *New From Selected,* or *Edit*. To create a new profile using an existing profile as a template, be sure to change the name of the profile you are editing before you save it.

Figure 7-1 Profile Editor



As you create or edit a profile, be sure to consider each of the following steps:

3. In the rules list, select the rule that you want to move, then click either Move Up or Move Down.

   One click moves the rule one place. Click the button as many times as needed to set the rule order.

   You can move more than one rule, but only one at a time.

4. Mark the check box next to any rule(s) you wish to use; unmark the check box for any rule(s) not to use. Because there are many rules, you can simplify this process by clicking Select All, and unmarking the ones you don't want, or by clicking Select None, then marking the ones you do want.

   Note: The check marks tell the program which rules to use, not the execution order of the rules.

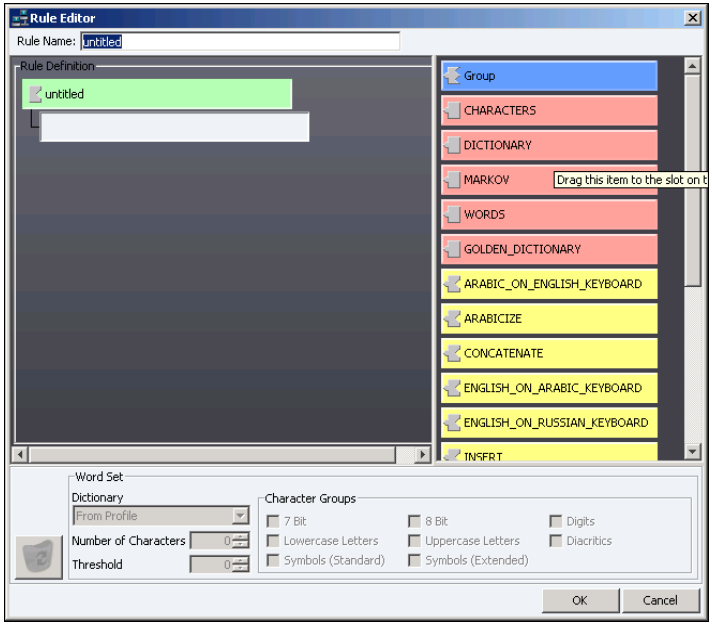
5. Click *OK*. The updated profile is saved and appears in the Manage Profiles List.
6. Click *Close* to close the Manage Profiles box.

Note: If you change the properties of a profile, such as modifying the rule order, the new changes are not applied to current jobs in the PRTK system. The changes are applied only to new jobs that are added.

UNDERSTANDING A USER-DEFINED RULE

You can create a user-defined rule to facilitate the decryption process for a file or set of files. You might create a password rule that combines dictionaries or adds certain prefixes or postfixes that might be relevant to the files. To use the password rule, you must then add it to a profile.

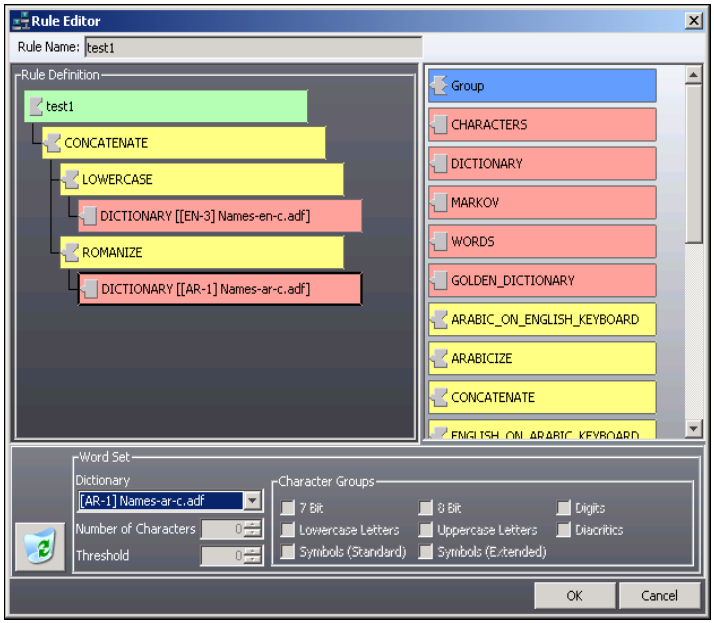
Figure 7-2 Creating a User-defined Rule



Use the Rule Editor to create or edit a rule. The types listed on the right side column of the Rule Editor are the building blocks for creating a rule. Types are different ways that

characters or words are permutated. Types and the information that you specify about the types are used to create rules.

Figure 7-3



One rule can have multiple types. For example, you can create a rule that combines words created by two different types, as seen in the graphic above.

In this example, the Lowercase type creates a lowercase word set of an English dictionary (en-u.adf). The Romanize type uses the words in an Arabic dictionary (ar-u.adf) to create a word set of Arabic words re-written with English letters. The Concatenate type then combines the two word sets created by the Lowercase and Romanize types to create a single word set.

Important: A word set is any series of words. Some word sets are stored in dictionaries, which are saved in (.ADF) files to your hard drive. It's available for use in multiple profiles and multiple sessions. Other words sets are not saved. For example, the Lowercase word set is generated by PRTK when the rule is applied, but the resulting word set is stored just in memory as the rule is being used.

Although you can combine types to create one rule, each type within the rule must ultimately point to a word set. The type uses the word set as its source to create a derivative word set.

In the example above, the Lowercase type uses an English dictionary as its source of words. The type applies its function of displaying all letters in the dictionary in lowercase letters. It then creates a new word set of lowercase English words.

The example above uses only English and Arabic dictionaries. However, you should generally create a user-defined rule that contains all dictionaries to increase the versatility of the user-defined rule. You can then specify the appropriate dictionaries in each profile.

The available basic word sets are:

- Characters
- Dictionary
- Markov
- Words (An exported word list from a forensic case, or from any other source)
- Golden Dictionary

Each word set and all available types can function either as sources or source modifiers.

A source is a word set or dictionary from which PRTK and DNA draw words.

TABLE 7-1 Available Word Sources and Descriptions

Source	Description
Character (source)	A word set based on a fixed-length sequence of characters. The character word sets are created from the languages specified in the profile. For example, you have created a profile that only uses the Spanish language. If you create a user-defined rule that contains the Character type, the character word set consists of only Spanish characters. If you select the Character type, you must enter the desired number of characters in the appropriate field, and you must check the character groups that you want to include.

TABLE 7-1 Available Word Sources and Descriptions

Source	Description
Dictionary (source)	A word set that is associated with a language. The entire set is tagged as codepage or UTF16-LE. Typically, when you create a user-defined rule, you only select this type when you need to specify a word set. This type doesn't perform any permutations of characters or words. If you select this type, you must select the dictionary from the Dictionary drop-down list, or select that dictionary in the Profile. Generally you should create a user-defined rule that contains all dictionaries to increase the versatility of the user-defined rule. You can then specify the appropriate dictionaries in each profile.
Markov (source)	The word set uses statistical Markov methods to create words with phonemes that sound like English words; however, the words themselves are actually meaningless. This is the only type that uses the Threshold field. The threshold number determines how many times any combination of letters must appear in a database table of all English words. If the combination of letters meets the threshold, then the letters are used to create words in the word set. A high threshold generates a relatively small number of words. A low threshold generates a large number of words.
Words (Source)	Words to be used with the modifiers. Type each word, or copy and paste a list of words. Each word must be followed by a hard return so it is on its own line in the list.
Golden Dictionary (source)	A word set that is not associated with a language and consists of previously discovered passwords. Each password is included in both code page and UTF16-LE. Typically, when you create a user-defined rule, you only select this type when you need to specify a word set. This type doesn't perform any permutations of characters or words.

A modifier is a word set that affects the source word set.

TABLE 7-2 Available Modifiers and Descriptions

Modifier	Description
Group (modifier)	A collection of types and their descriptions. Use the Group type to save a collection of types to apply to other user-defined rules.

TABLE 7-2 Available Modifiers and Descriptions

Modifier	Description
Arabic on English Keyboard (modifier)	Transforms Arabic words typed on an English keyboard into English words that might be passwords. The words are created according to the key location on the keyboard. For example, this type replaces the letter "shin" in Arabic with the letter "a" in English because they have the same location on a keyboard. The new English words are completely meaningless. If you select this type, you must create a subordinate Character, Dictionary, Golden Dictionary, or Markov type.
Arabicize (modifier)	Uses a word from any non-Arabic language and replaces the letters in the word with the corresponding letters in the Arabic alphabet; "alif" replaces "a" for example. If you select this type, you must create a modifier.
Concatenate (modifier)	Combines words from different word sets. This type takes one word from one word set and places it next to one word from another word set. For example, if one word set consists of dog and the other word set consists of cat, the Concatenate type creates "dogcat" and "catdog." If you select this type, you must create two subordinate Character, Dictionary, Golden Dictionary, or Markov types.
English on Arabic Keyboard (modifier)	Transforms English words typed on an Arabic keyboard into Arabic words that might be passwords. The words are created according to the key location on the keyboard. For example, if you've memorized a password by keystroke, the password will be the same between different keyboards.
English on Russian Keyboard (modifier)	Transforms English words typed on an Russian keyboard into Russian words that might be passwords. The words are created according to the key location on the keyboard. For example, if you've memorized a password by keystroke, the password will be the same between different keyboards.
Insert (modifier)	Places each word of one word set into all possible positions for each word in another word set. For example, if the word set consists of dog and cat, the Insert type creates cdogat, cadogt, catdog, and so on. If you select this type, you must create a subordinate Character, Dictionary, Golden Dictionary, or Markov type.

TABLE 7-2 Available Modifiers and Descriptions

Modifier	Description
Lowercase (modifier)	Uses an existing word set to create another word set that is all lowercase letters. If you select this type, you must create a subordinate Character, Dictionary, Golden Dictionary, or Markov type.
Multi-slot (modifier)	Allows multiple passwords on one file. This type is only used for the DriveCrypt and DriveCrypt Plus Pack. If you select this type, you must create a subordinate Character, Dictionary, Golden Dictionary, or Markov type.
Primary (modifier)	Uses a word set and performs the following for each word in that set: • Lowercased • Uppercased • Lowercased with the first letter uppercased • Uppercased with the first letter lowercased If you select this type, you must create a subordinate Character, Dictionary, Golden Dictionary, or Markov type.
Reverse (modifier)	Uses a word set and reverses each word in the set. If you select this type, you must create a subordinate Character, Dictionary, Golden Dictionary, or Markov type.
Romanize (modifier)	Uses Arabic words and replaces letters according to the sounds of English letters. If you select this type, you must create a subordinate Character or Dictionary type. If you select the Character type, the profile must include the Arabic language. If you select the Dictionary type, you must select an Arabic dictionary.
Russian on English Keyboard (modifier)	Transforms Russian words typed on an English keyboard into English words that might be passwords. The words are created according to the key location on the keyboard. For example, if you've memorized a password by keystroke, the password will be the same between different keyboards.
Secondary (modifier)	Uses a word set to create another word set of both lower- and uppercased words. If you select this type, you must create a subordinate Character, Dictionary, Golden Dictionary, or Markov type.

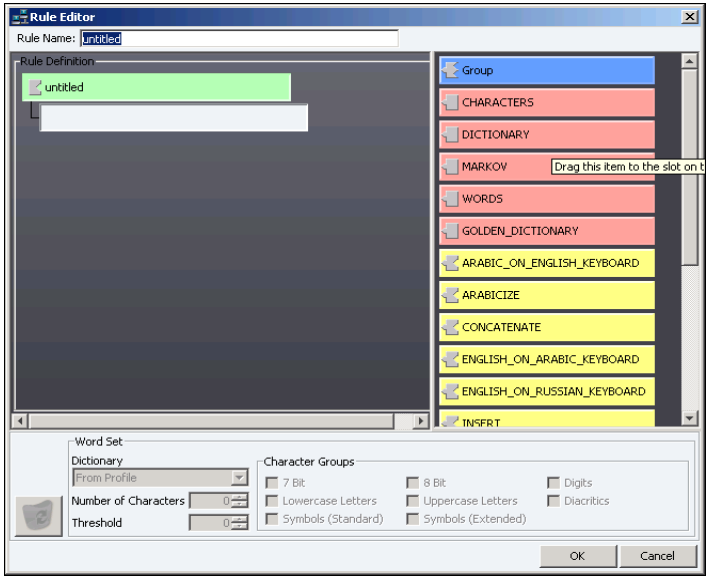
TABLE 7-2 Available Modifiers and Descriptions

Modifier	Description
Two Uppercase (modifier)	Uses a word set and creates another word set that uppercases one and two letters at a time for each word. If you select this type, you must create a subordinate Character, Dictionary, Golden Dictionary, or Markov type.

CREATING A USER-DEFINED RULE

You can use the Rule Editor form to create a user-defined rule. In doing so, until you are comfortable with the process, you might want to put on paper what you want to accomplish, then work backwards on your paper list as you create the rule from the top down. Notice the shaped icons to the left of each item type in the column on the right. The shapes indicate which items fit with other items as you combine them.

Figure 7-4 Using the Rule Editor



The following table describes the Word Set options at the bottom of the Rule Editor form:

TABLE 7-3 Word Set Options and Descriptions

Option	Description
Type	The basic unit of a user-defined rule. You can select multiple equal or subordinate types per rule.
Dictionary	The available dictionaries. You only use this drop-down list when you select a Dictionary type. Generally you should create a user-defined rule that contains all dictionaries to increase the versatility of the user-defined rule. You can then specify the appropriate dictionaries in each profile.
Number of Characters	The number of characters to include in a character word set. You only use this field when you select a Character or Markov type.
Threshold	The number of times a combination of letters must be found to include it in the Markov word set. You use this field only when you select the Markov type.
Character Groups	The following are specific character groups to use in the Character word set: • All 7-bit Characters (ASCII): Searches for any ASCII characters. This box includes all characters listed above it. • All 8-bit Characters: Searches for any ASCII and Extended ASCII characters. This box includes all characters listed above it and the Extended ASCII characters. • Digits: Searches for numbers. • Lowercase Letters: Searches for lowercase letters. • Uppercase Letters: Searches for uppercase letters. • Diacritics: Searches for diacritics, such as the tilde (~) or the circumflex (^). • Symbols (Standard): Searches for symbols that are available on a standard keyboard, such as the plus sign (+) or the dollar sign ($). • Symbols (Extended): Searches for symbols from the ASCII character set, 0-255. Use this list only if you select the Character type.

To create a user-defined rule:

1. Select *Edit* > *Rules* > *New*.
2. Enter the name of the new user-defined rule.

You might name the rule according to its function, such as Combine Arabic/ English words.

3. Build the rule using the Sources and Modifiers available.
4. Refine the rule based on the Sources and Modifiers selected.
5. To add an additional type at the root rule, select the rule name and then click *Add*.
6. To remove any type in the hierarchy, select the type in the Hierarchy window and click *Remove*.
7. Click *OK*. Click *Cancel* if you do not want to save the information you entered on the form.

EDITING A USER-DEFINED RULE

You might want to edit a user-defined rule to increase the effectiveness of the rule. You can modify any of the information that you specify when you create a new rule, such as the rule name and the types used in the rule.

To edit a user-defined rule:

1. Select *Edit* > *Rules*.
2. In the User-defined Rules screen, select the rule that you want to modify and then click *Edit*.
3. Enter the new information in the Rule Editor form.
4. Click *OK*.

   Click *Cancel* if you do not want to save the information you entered on the form.

REMOVING A USER-DEFINED RULE

You might delete a user-defined rule if you no longer need its functionality in the files that you are processing.

You delete a rule on the User-defined Rules form. To delete a user-defined rule:

1. Select *Edit* > *Rules*.
2. In the User-defined Rules screen, select the rule that you want to delete.
3. Click *Remove* > *Yes*.

Chapter 8 Using the Dictionary Utility

PRTK 6.5 and DNA 3.5 use dictionaries to identify possible passwords. You can create, import, and browse the dictionaries.

Note: After you create or import any dictionary, you must add the dictionary to a profile. For more information, see "Editing a Profile" on page 99.

DICTIONARY BASICS

PRTK and DNA use dictionaries to discover the passwords that decrypt files. The dictionary attacks employ the default dictionaries included with the product as well user-defined biographical and other custom user dictionaries.

PRTK and DNA automatically store recovered passwords in a single file referred to as the Golden Dictionary. This file contains all recovered passwords (in both code page and Unicode) from all PRTK jobs. The Golden Dictionary is automatically created after PRTK recovers its first successful password.

Biographical dictionaries contain personal data, such as dates or phrases, significant to the person who created the password. Most passwords used with general applications contain some information about the person who locked the file. Therefore, creating a dictionary that contains personal data on the person in question increases the probability that you can recover the password.

User dictionaries contain key phrases or words that are associated with the investigation but not with the person who locked a particular file.

Note: To create a user dictionary, enter one word per line in a standard text editor such as Notepad. Each term must be separated with a hard return.

PRTK and DNA support dictionaries in Arabic, English, French, German, Italian, Russian, and Spanish. All dictionaries for both programs are stored by default in

[*drive*]:\Documents and Settings\All Users\Application Data\AccessData\PR\Dictionaries.

During a dictionary attack, PRTK and DNA use the information in the selected profile to create variations, permutations, and combinations of the biographical and user dictionaries. Additionally, it uses phonetic alterations, adds prefixes or suffixes, and substitutes characters.

By default, PRTK and DNA use the following dictionaries in this order:

1. The Golden Dictionary
2. Biographical dictionary/As-is dictionaries
3. Those specified in the profile

PRTK & DNA DICTIONARY UTILITY

Dictionaries are an optimization tool used for password recovery. By using dictionaries, specific candidate passwords are tested before the more general ones. This utility creates a variety of custom dictionaries for use with both PRTK and DNA.

Make backup copies of word lists and dictionaries before using this utility. Once a dictionary has been modified or deleted, there may be no way to recover it.

STARTING THE DICTIONARY UTILITY

Use the Dictionary Utility to create or modify several types of dictionaries.

To start the Dictionary Utility:

1. Start either PRTK or DNA.
2. Click *Tools* > *Dictionary Tools*.
3. From the AccessData Dictionary Import Utility screen that appears, click *Dictionary Tools*.
4. Select which tool to use.

The following table lists tools can be accessed from the Dictionary Tools menu, and their functions. Each is covered in more detail in this chapter.

TABLE 8-1 Available Dictionary Tools

Tool	Function
Dictionary Browser	Provides a way to view the words in each dictionary, or to delete a particular dictionary or dictionaries.
Dictionary Info	Provides a way to see the specific details about a dictionary, such as the dictionary type, encoding, language, word count, and a description.
Biographical Dictionary Generator	Builds dictionaries of candidate (possible) passwords from a collection of biographical details and from combinations of the biographical data entered.
Pass-phrase Dictionary Generator	Builds dictionaries from a phrase file and by using sub-phrases from the phrase file.
Permutation Dictionary Generator	Builds dictionaries from a wordlist file and by using permutations of words from the wordlist file.
Standard Dictionary Generator	Builds custom dictionaries using a wordlist file. The Standard Dictionary Generator is the default window that appears in the AccessData Dictionary Import Utility
Golden Dictionary Merge	Merges two golden dictionaries into a single golden dictionary. It also converts golden dictionaries from PRTK 5 and DNA 2 into the current golden dictionary format.

When completed successfully, the dictionary tool generates both Code-page and a Unicode format dictionaries that you will find in the following directories:

- Documents and Settings\All Users\Application Data\AccessData\PR\Dictionaries

BROWSE DICTIONARIES

The Browse Dictionaries tool provides a way to view the contents of a dictionary, or to delete a dictionary. Use the mouse to select a dictionary file from the list of those found in the current directory.

- When you select a dictionary, click *View Entries* to see a window containing a scrollable list of the dictionaries entries.
- Use the scroll bar to move up or down the list. When you select a dictionary and click the Delete button, a confirmation dialog opens to make sure you really want to delete the file.

Important: You cannot recover a deleted dictionary. Be careful when deleting!

DICTIONARY INFORMATION

The Dictionary Information tool provides a way to view details about an AccessData dictionary. The interface is divided into two different areas: the Dictionaries list and navigation controls and the Details panel.

The navigation controls allow you to navigate your hard disk to the dictionaries that you have. Selecting a dictionary in the navigator displays the details for that dictionary in the details panel below. The navigator window shows only dictionary files and directories. Each dictionary file entry shows the filename, type, word count, and the date the file was last modified.

The Details Panel shows the following information:

TABLE 8-2 Detailed Dictionary Information

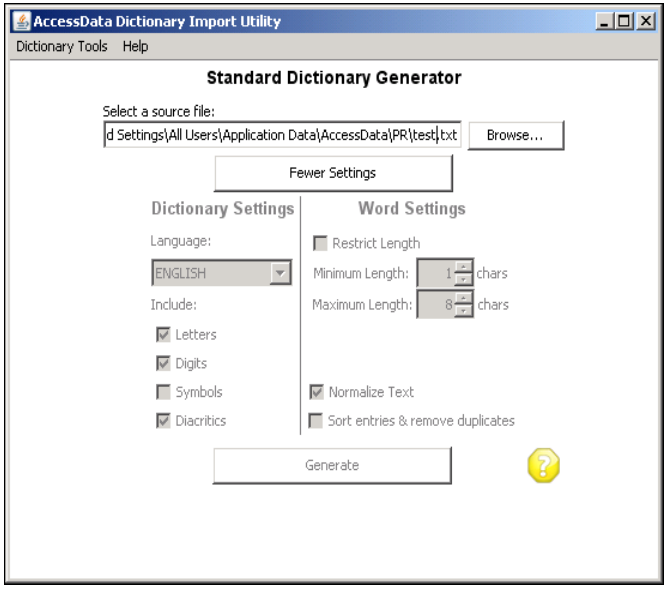
Information	Description
Encoding	Codepage indicates a standard 8-bit character encoding; UTF-16LE indicates a 16-bit little-endian encoding. Only these encodings are supported at this time.
Language	The special vocabulary and usages of a scientific, professional, or national group.
Word Count	The number of words the dictionary actually has as counted by the Dictionary info tool.
Description:	An explanation of the selected dictionary's contents, if one was entered when the dictionary was created.

STANDARD DICTIONARY GENERATOR

The Standard Dictionary Generator tool provides a way to create standard dictionaries from a source list of words. You can enter the full path or browse to the source word

list file. Once a file has been selected, the remainder of the controls will become available.

Figure 8-1 Generating a Standard Dictionary



A source word list is provided in a text file where each word is separated from the others by a hard return. You can use a phrase in place of a word since the tool does not try to separate the provided text, except at carriage returns.

Under the dictionary settings the language for the dictionary as well as the type of characters that occur in the dictionary can be specified. By unchecking one of the character types, that character type will be filtered from the phrases added to the dictionary.

The tool filters these character types:

TABLE 8-3 Dictionary Settings

Dictionary Settings	Description
Language	Choose the language in which to generate the dictionary.

TABLE 8-3 Dictionary Settings

Dictionary Settings	Description
Include	Check to Include, or uncheck to exclude the following character types: **Letters:** Alphabetic characters used to compose words. These include letters with diacritic marks and any other type of composed character used to construct words. **Digits:** Numeral characters (0–9). **Symbols:** Symbol characters. These include punctuation and non-alpha or digit characters, but do not include the diacritic marks used for composed characters. **Diacritics:** The special characters used in composed characters. If letters are included but diacritics are not, then the base letter will be preserved.

Use the following word settings to further refine your dictionary:

TABLE 8-4 Word Settings

Word Setting	Description
Restrict Length	If the check box to restrict the length is checked, then the maximum length of each word, in characters can be specified. The permutation will be truncated to the specified length regardless of the resulting number of words that will remain in the generated permutation. Options: • Minimum word length • Maximum word length
Normalize Text	Standardizes all words in lowercase format.
Sort entries & remove duplicates	Sorts all entries in the word list and removes duplicates to minimize search time.

When the dictionary generation is successfully completed, two dictionaries will have been created, one each for Unicode and Codepage encodings.

BIOGRAPHICAL DICTIONARY

The Biographical Dictionary tool creates dictionaries using personal data such as dates or phrases about the suspect.

BIOGRAPHICAL DICTIONARY DATA

Since people use passwords that are easy to remember, the passwords often take the form of something meaningful to the person creating the password.

Just as a homeowner might invest in a high-quality door lock and then hide a key under the doormat, a computer user might install sophisticated encryption technology and then use glaringly obvious passwords:

- Names, dates, phone numbers, and addresses
- Birthdays, anniversaries, or other significant dates
- Interests and hobbies
- Pets, celebrities, family
- Favorite books, movies, songs, poems
- Social Security Numbers

You can also glean valuable personal details for the biographical and user dictionaries by evaluating the physical evidence at an investigation site. Often the routine clues—sticky notes, phone number lists, date books, electronic lists (perhaps in a file named "passwords" on a hard drive or floppy disk), entries on a Palm Pilot/Pocket PC, or even a file on a thumb drive or the Compact Flash card in a digital camera—offer valuable information. Hiding places can range from the most ingenious to right out in plain sight. Be careful not to overlook the obvious.

The following can provide valuable clues at a crime scene:

- Books and magazines
- Photographs
- Calendars, day planners, and personal organizers
- Notes and mail, including e-mail
- Paraphernalia

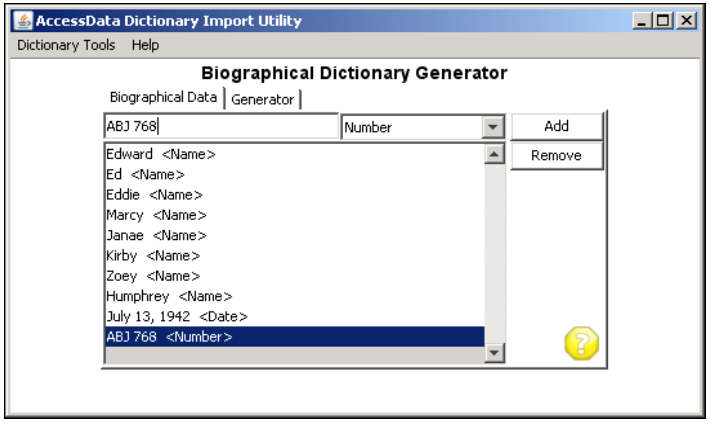
In addition, reconstructing the alleged crime or using related evidence found at the scene can give the investigator clues which can be leveraged in the biographical dictionary. Additional clues can be observed by how the evidence interacts, how the suspect uses digital media, or how the times are related to evidence and events.

To understand how evidence relates to the crime, the investigator must evaluate the geographic location of people and computers as well as any communication or transactions that occurred between them. For example, in a fraud investigation involving thousands of people and computers, understanding where each party was

located and how they interacted can reveal important information about the biography of the criminal. Sorting the financial transactions of individuals or organizations can also reveal patterns of behavior.

By observing the evidence at a scene and reconstructing the actions performed by the subject, you can create a more effective word list to be used in generating the biographical dictionary.

Figure 8-2 Using the Biographical Data Tab



You can enter words or numbers in the Word field, such as the name of the individual that you are creating the dictionary about and the birthdate.

The Data drop-down menu lists the following types of personal information:

TABLE 8-5

• Name	• ZIP Code	• Number
• Address	• Country	• Word
• City	• Phone Number	• Phrase
• State	• Date	

Any combination and arrangement of the information you can think of will make your biographical dictionary more effective. Make every guess you can at a subject's password, and enter as many versions of the guess as you can.

You can use a variety of different formats to enter numeric information, such as phone number and date. For example, you can enter a phone number as 111.222.3334 or 111–222–3334. Enter as many different formats as you can think of.

To create a biographical dictionary:

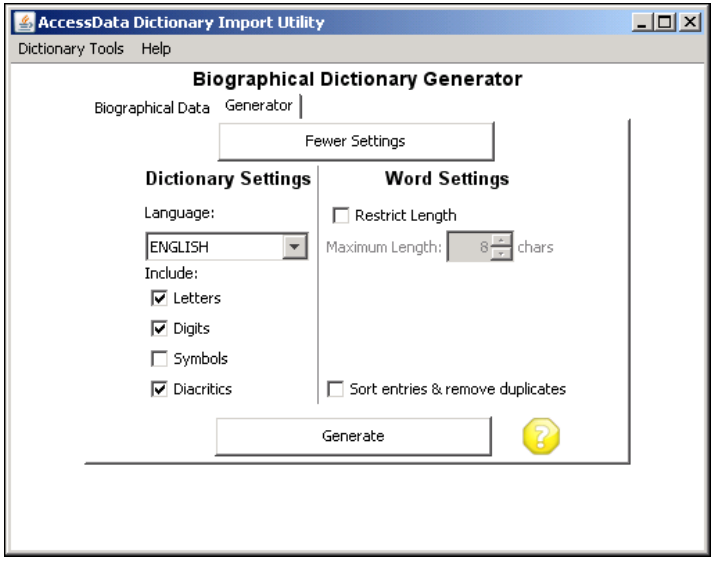
1. Select *Tools* > *Dictionary Tools* > *Dictionary Tools* > *Biographical Dictionary Generator*.
2. Click the *Biographical Data* tab.
3. In the Data drop-down list, select the type of personal data to enter.
4. Type the personal data into the Word field, then click *Add*, or press Enter.

   To remove a word and its type from the Word list, select the word and click the *Remove* button.
5. Click the *Generator* tab to create a dictionary based on the Word list, then specify your dictionary and word settings.
6. Click *More Settings* to see all available options,

   OR

   Click *Fewer Settings* to close the options field.
7. When you have finished adding your word list and specifying settings for this dictionary, click *Generate*, and enter the name of the biographical dictionary.

Figure 8-3 Using the Biographical Dictionary Generator Tab



The biographical dictionary is automatically added to the list of dictionaries in PRTK in codepage (-c), Unicode (-u), and as-is (-xml) formats.

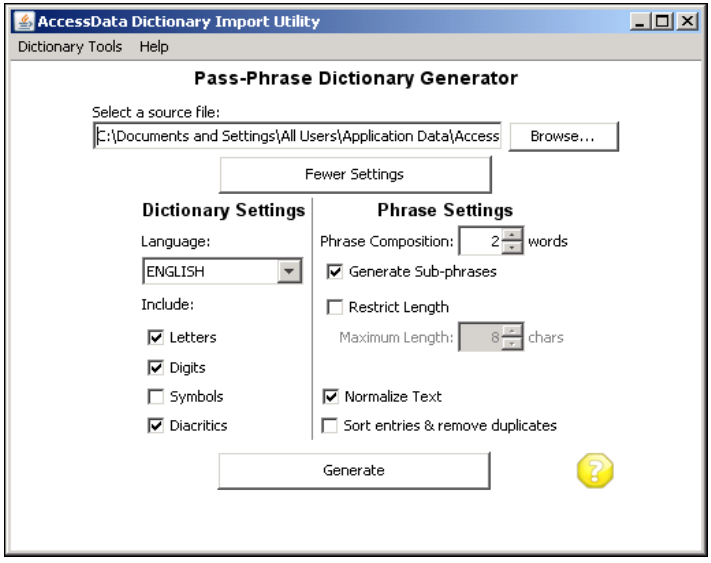
PASS-PHRASE DICTIONARY GENERATOR

A pass-phrase is a password phrase composed of some number of consecutive words from a provided source phrase. The tool generates all phrases from two words up to the configuration length specified in the user interface by working through the source phrase from start to finish. Source phrases are provided to the tool in a text file where each phrase is separated from the others by a hard return.

To create a pass-phrase dictionary:

1. Select *Tools* > *Dictionary Tools* > *Dictionary Tools* > *Pass-phrase Dictionary Generator*.
2. Click *More Settings* to open the Dictionary Settings and Phrase Settings view.

Figure 8-4 Using the Pass-Phrase Dictionary Generator



3. Make your Dictionary Settings and Phrase Settings selections based on the information in the tables below.
4. When you are satisfied with the settings you have selected, click *Generate*, and name your dictionary.

Use the Dictionary Settings to specify the language and character types to use in generating this dictionary, according to the information in the following table:

TABLE 8-6 Dictionary Settings

Dictionary Settings	Description
Language	Choose from thirty languages that PRTK/DNA has dictionaries for, according to what will produce the most likely useful results.
Include	Check to Include, or uncheck to exclude the following character types to be included in the Pass-Phrase:
	Letters: Alphabetic characters used to compose words. These include letters with diacritic marks and any other type of composed character used to construct words.
	Digits: Numeral characters (0–9).
	Symbols: Symbol characters. These include punctuation and non-alpha or digit characters, but do not include the diacritic marks used for composed characters.
	Diacritics: The special characters used in composed characters. If letters are included but diacritics are not, then the base letter will be preserved.

Use the Phrase Settings to narrow or broaden your pass-phrase dictionary contents as described in the following table:

TABLE 8-7 Phrase Settings

Setting	Description
Phrase Composition	Specify the maximum number of consecutive words to use for each generated phrase. If the requested number of words is more than the total number of words in the source phrase, then the entire source phrase will be used.
Generate Sub-phrases	For each phrase in the list, Generate
Restrict Length	Specify the number of characters to include in each phrase. This is deactivated by default.
	If checked, you can specify the maximum length of the phrase in characters. The generated phrase will be truncated to the specified length regardless of the resulting number of words that will remain in the generated phrase.
Normalize Text	Standardizes all words in lowercase format.
Sort entries & remove duplicates	Sorts all entries in the word list and removes duplicates to minimize search time.

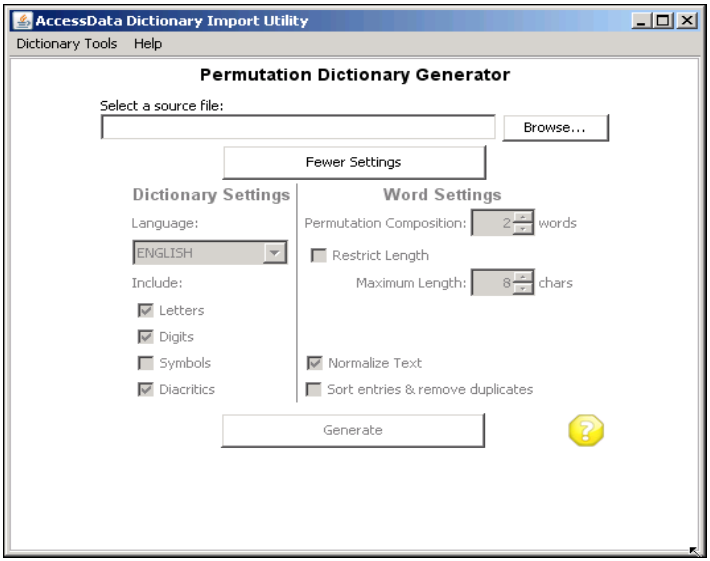
PERMUTATION DICTIONARY GENERATOR

A permutation is simply some combination of words from a specified source list where each word is used once in the resultant sequence. This tool will generate all possible permutations from one to the number of words specified as the configuration in the user interface.

To create a Permutation dictionary:

1. Click *Tools* > *Dictionary Tools*.
2. Click *Dictionary Tools* > *Permutation Dictionary Generator*.
3. Click *More Settings* to open the Dictionary Settings and Word Settings view.

Figure 8-5 Creating a Permutation Dictionary



4. Make your selections from the available Dictionary and Word settings, according to the tables below.
5. When satisfied with your selections, click Generate.

This tool provides a way to create dictionaries of the various permutations, or ordered combinations of a source list of words. If you have a source word list file, you can enter the full path or browse to the file. Once a file has been selected, the remainder of the controls will become available.

Use the Dictionary Settings for the following tasks:

TABLE 8-8 Dictionary Settings

Dictionary Settings	Description
Language	Choose from thirty languages that PRTK/DNA has dictionaries for, according to what will produce the most likely useful results.
Include	Check to Include, or uncheck to exclude the following character types to be included in the Pass-Phrase
Letters	Alphabetic characters used to compose words. These include letters with diacritic marks and any other type of composed character used to construct words.
Digits	Numeral characters (0–9).
Symbols	Symbol characters. These include punctuation and non-alpha or digit characters, but do not include the diacritic marks used for composed characters.
Diacritics	The special characters used in composed characters. If letters are included but diacritics are not, then the base letter will be preserved.

You can use a phrase in place of a word since the tool does not try to separate the provided text, except at carriage returns. In a source word list each word is separated from the next by a hard return in a text file saved in UTF-8 or Unicode format.

You can specify the language for the dictionary as well as the type of characters that occur in the dictionary under the dictionary settings. By unchecking one of the character types, that character type will be filtered from the phrases added to the dictionary.

Use the Word Settings to narrow or broaden your permutation dictionary contents as described in the following table:

TABLE 8-9 Word Settings

Setting	Description
Permutation Composition	Specify the maximum number of consecutive words to use for each generated phrase. If the requested number of words is more than the total number of words in the source phrase, then the entire source phrase will be used.

TABLE 8-9 Word Settings

Setting	Description
Restrict Length	Specify the number of characters to include in each phrase. This is deactivated by default.
	If checked, you can specify the maximum length of the phrase in characters. The generated phrase will be truncated to the specified length regardless of the resulting number of words that will remain in the generated phrase.
Normalize Text	Standardizes all words in lowercase format.
Sort entries & remove duplicates	Sorts all entries in the word list and removes duplicates to minimize search time.

MERGE GOLDEN DICTIONARIES

Two dictionaries are needed in order to perform a merge: a source and a target.

The source dictionary can be either a 5.x or 6.x golden dictionary, while the target dictionary must be a 6.x golden dictionary.

When you click the merge button, the contents of the source dictionary are written into the target dictionary. The utility will display the following information:

- Passwords Merged: the number of passwords added from the source dictionary to the target dictionary to create the new golden dictionary

  Note: The Merge Golden Dictionary tool does not add duplicate passwords to the new dictionary.

- Total Passwords: the number of passwords contained in the new golden dictionary.

Chapter 9 Specialized Password Recoveries

This chapter reviews the steps required to perform specialized password recoveries using PRTK 6.5, and DNA 3.5.

RECOVERING LOGIN PASSWORDS

PRTK and DNA can recover the user login password from Windows NT 4.*x*, 2000, and XP, and Vista systems. For Windows NT 4.x, 2000, and XP, these passwords are located in the SAM file and System file found in the following directory:

[*drive*]:\Windows_directory\system32\config\

Windows locks the SAM file and system file, so they cannot be directly accessed through the operating system. Use FTK Imager to access these files.

ACCESSING THE SAM FILE AND THE SYSTEM FILE

To access the SAM file and system file, you must do one of the following:

- If you are using FTK Imager, export the SAM file and system file.

  FTK Imager bypasses the Windows operating system, allowing you to copy the Windows-locked files. The only potential problem is that if the SAM file and system file are being written to during the copy operation, you may get a corrupted copy. For instructions on using FTK Imager to obtain the necessary files, see "Recovering Login Passwords on Windows 2000 and XP Systems" on page 133.
- If you have an image, extract the SAM file and the System file from the [*drive*]:\Windows_directory\system32\config\ directory and save them to a

temporary folder on the password recovery hard drive. Follow steps 7 and 8 under "Recovering Login Passwords on Windows 2000 and XP Systems" on page 133.

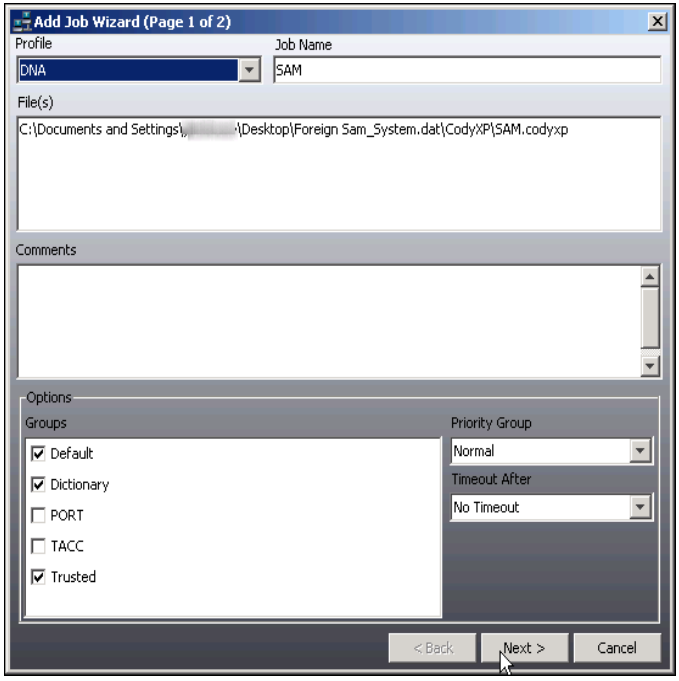
- If you are not using FTK Imager or if you do not have an image, boot your computer from a boot disk and copy the SAM file and the System file from the system drive. For more information on how to obtain the necessary files using a boot disk, see "Recovering Passwords Using a Boot Disk to Access the Files" on page 133.

Recovering Login Passwords from Windows NT

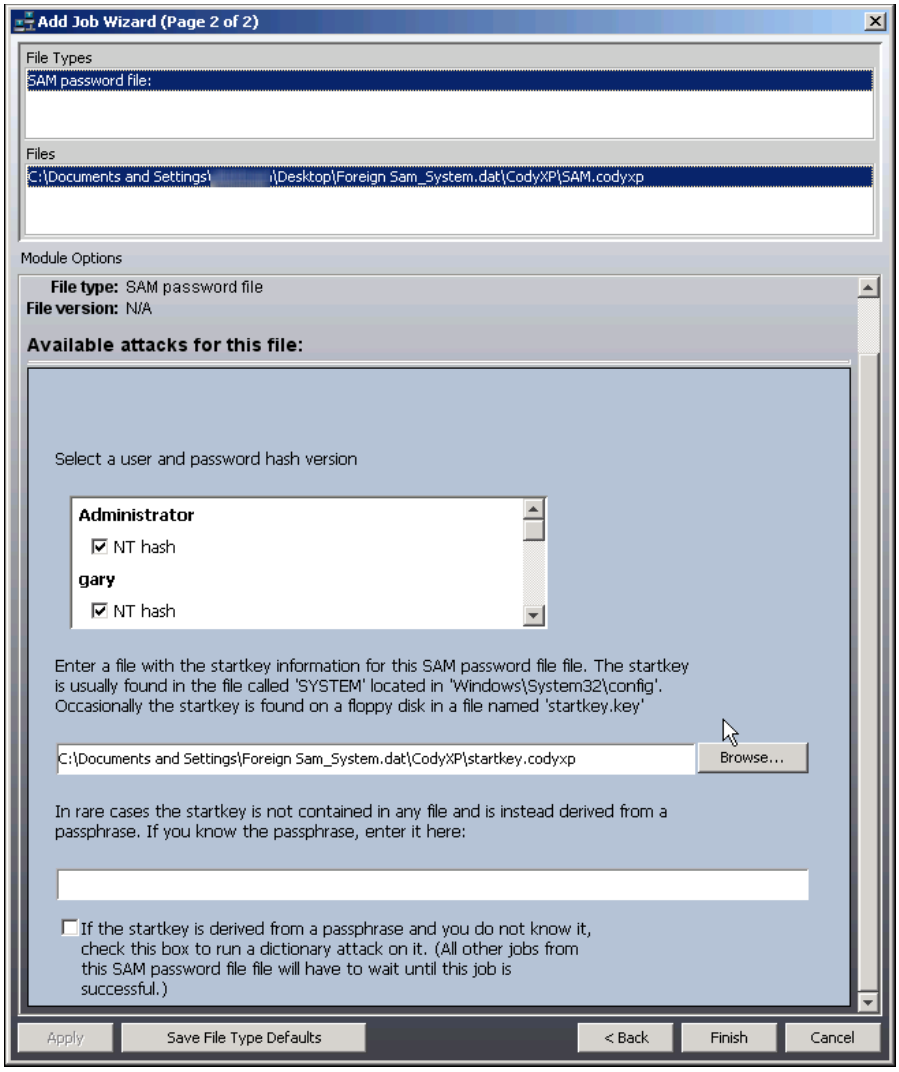
When the source of the password files is Windows NT (not NT 4 SP3 or later), you must perform the password recovery on a Windows 2000, XP, or Vista system, after you obtain the SAM file and the System file:

1. Copy the SAM file and the System file to a temporary medium to transfer them to a machine with the appropriate operating system.
2. Run PRTK or DNA.
3. Select *Edit* > *Add Files*, and then browse to and select the SAM file, or drag and drop the SAM file into the PRTK or DNA Window.

   The Add Job Wizard (Page 1 of 2) opens. Select the Profile, worker Group(s), Priority Group, and Timeout After settings to use for this job.



4. Click *Next*.


Add Job Wizard (Page 2 of 2)
File Types
SAM password file:
Files
C:\Documents and Settings\ \Desktop\Foreign Sam_System.dat\CodyXP\SAM.codyxp
Module Options
File type: SAM password file
File version: N/A
Available attacks for this file:
Select a user and password hash version
Administrator
NT hash
gary
NT hash
Enter a file with the startkey information for this SAM password file file. The startkey is usually found in the file called 'SYSTEM' located in 'Windows\System32\config'. Occasionally the startkey is found on a floppy disk in a file named 'startkey.key'
C:\Documents and Settings\Foreign Sam_System.dat\CodyXP\startkey.codyxp
Browse...
In rare cases the startkey is not contained in any file and is instead derived from a passphrase. If you know the passphrase, enter it here:
If the startkey is derived from a passphrase and you do not know it, check this box to run a dictionary attack on it. (All other jobs from this SAM password file file will have to wait until this job is successful.)
Apply
Save File Type Defaults
< Back
Finish
Cancel

5. In the Add Job Wizard (Page 2 of 2), under Module Options, click in the check boxes under each user's name, next to the attack types you wish to run for each user. Unmark the check boxes for jobs listed under users whose information you do not need.

   Below the attack types box you will see a Browse button next to a box that should be filled with the path and filename for the System or the Startkey file that matches the user and the system the SAM file is from.

6. Click *Browse* to automatically open the same folder the SAM file was added from.
7. Select the appropriate System file or syskey file, then click *Open*.
8. The startkey field in the Add Job Wizard (Page 2 of 2) should now be populated with the correct information.
9. Click *Finish*.
10. PRTK and DNA analyze the SAM file and System file and recover the login password. Since there can be multiple users in the SAM file and the System file, each with a unique password, multiple SAM file jobs may be added to the job list —once for each user found and selected and each attack type chosen for each user selected.

RECOVERING PASSWORDS FROM WIN 9X FILES

PRTK and DNA can recover passwords from PWL files. PWL files are specific to Windows 9.*x* systems and are typically located in the [*drive*]:\Windows directory. They contain user-specific passwords for items such as the following:

- Mapped drive passwords
- Dial-up networking passwords
- Secure website login passwords

Important: PRTK and DNA do not run on Windows 9.*x* systems. You cannot recover PWL files directly from their native environment. You must copy them to a Windows XP, 2003 or Vista system.

A separate PWL file exists for each user on the current system. The actual filename is an 8.3 derivative of the user's login name (for example, roy.pwl or elizabet.pwl).

To determine the user's login name, check the system.ini folder in the Windows directory. The system.ini folder lists the login names of every user on the current system.

After you have determined the user's login name, you can drag and drop the PWL file into the PRTK or DNA Job List pane. When PRTK or DNA attempts to recover the passwords in the PWL file, it prompts you for the user's login name. PRTK or DNA then retrieves the passwords within the file.

Recovering Login Passwords on Windows 2000 and XP Systems

On Windows NT 4 SP3 and later, Windows 2000, and Windows XP systems, PRTK and DNA must first have the SAM file and the appropriate System file before it can find the login passwords in the SAM file and System file.

By default, the syskey is stored locally in the System registry file located in the [drive]:\Windows_directory\system32\config\ directory. The syskey is a utility that encrypts the hashed password information in a SAM database using a 128-bit encryption key.

Important: If the syskey is stored in the System registry file, it cannot be directly accessed because, like the SAM file and System files, Windows keeps it locked. Otherwise, the syskey could be stored on a floppy disk.

To extract the SAM file and the System file from a live system that is not your PRTK or DNA password recovery system, do the following:

1. Install FTK Imager on the local hard drive, or copy the files from a system where it is installed to a thumb drive and connect that to the live system you want to extract the SAM file and the System file from.
2. Run FTK Imager.
3. In the toolbar, click the Obtain Protected Files button
4. Under Options, choose either *Minimum files for login password recovery*, or *Password recovery and all registry files*, according to your needs.
5. Specify the location to save the extracted files to.

   If you have a thumb drive, a portable drive, or a network directory available, save the files to a new folder there so you can take them to the system where you will be doing the password recovery.
6. Click OK to close the dialog and run the extraction. When complete, close FTK Imager.
7. Connect the portable drive to the recover system, and copy the files to the hard drive where PRTK or DNA is running.

For information on processing the extracted or collected files, see "Processing the Protected System Files in PRTK or DNA" on page 134.

Recovering Passwords Using a Boot Disk to Access the Files

To boot your computer from a boot disk and copy the System registry file:

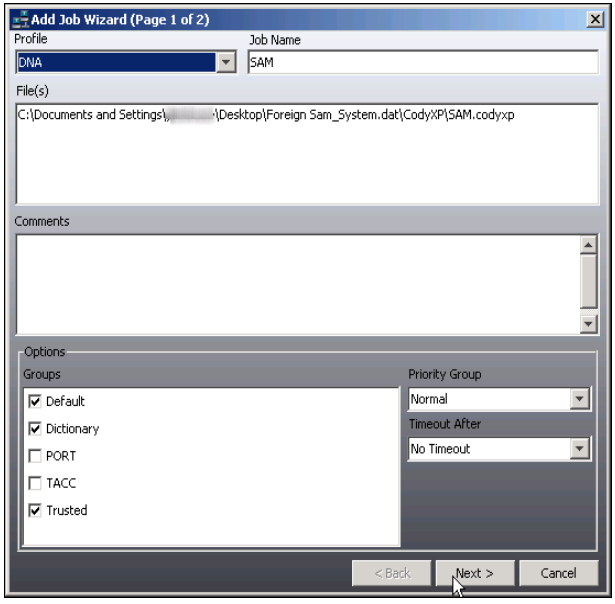
1. Restart the computer with a boot disk that is able to read your system drive.

   If the system drive is a FAT partition, you can use a Windows 98 boot disk. If the system drive is an NTFS partition, you must use a Linux or NTFSDOS boot disk.
2. After booting to the boot disk, go to the [drive]:\Windows_directory\System32\config\ directory.
3. Copy the SAM file and System file to another location, such as a floppy disk or a network directory.
4. Restart the computer normally.

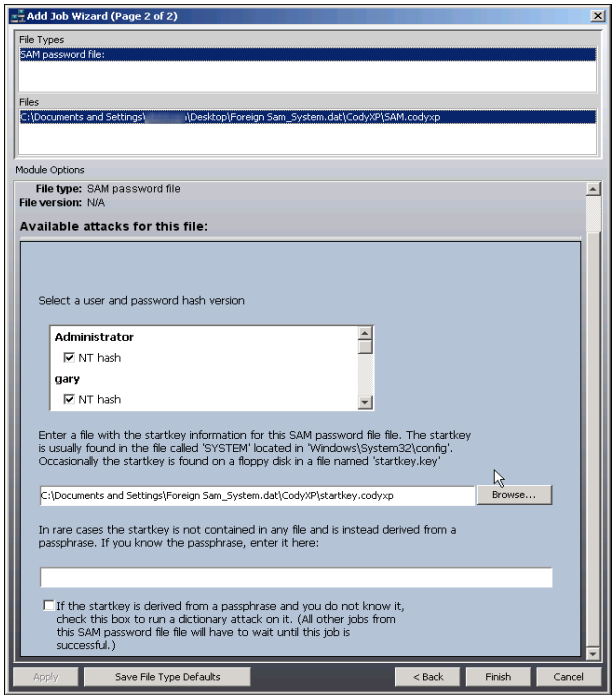
PROCESSING THE PROTECTED SYSTEM FILES IN PRTK OR DNA

To add the SAM file and System file as jobs in PRTK or DNA, after obtaining them:

1. Add the SAM file to PRTK or DNA. If the System file is stored in the same folder as the SAM file, and your recovery is running on the same machine as the source files, will be read and referenced automatically. If the Protected System Files have been obtained from another machine, add the SAM file, and you will be prompted on the second page of the Add Job Wizard for the location of the System file; it does not need to be added as a separate job.



2. Specify the module options.


Add Job Wizard (Page 2 of 2)
File Types
SAM password file:
Files
C:\Documents and Settings\ \Desktop\Foreign Sam_System.dat\CodyXP\SAM.codyxp
Module Options
File type: SAM password file
File version: N/A
Available attacks for this file:
Select a user and password hash version
Administrator
NT hash
gary
NT hash
Enter a file with the startkey information for this SAM password file file. The startkey is usually found in the file called 'SYSTEM' located in 'Windows\System32\config'. Occasionally the startkey is found on a floppy disk in a file named 'startkey.key'
C:\Documents and Settings\Foreign Sam_System.dat\CodyXP\startkey.codyxp
Browse...
In rare cases the startkey is not contained in any file and is instead derived from a passphrase. If you know the passphrase, enter it here:
If the startkey is derived from a passphrase and you do not know it, check this box to run a dictionary attack on it. (All other jobs from this SAM password file file will have to wait until this job is successful.)
Apply
Save File Type Defaults
< Back
Finish
Cancel

3. Click *Browse* to specify the location of the System or the startkey.key file.

   - If the System file is on a hard drive or a network drive, browse to and select the System file to add it to the Available Attacks For This File dialog.
   - If the computer requires a floppy disk to authenticate, select the startkey.key file from the floppy. If you do not specify the syskey, the syskey for the local machine is used.

   Note: Without a valid System file or startkey.key file, the password cannot be recovered.

RECOVERING PASSWORDS FROM THE WINDOWS REGISTRY

The Windows registry is essentially a set of data files that Windows uses to control hardware, software, user information, and the overall functionality of the Windows interface. Registry files are particularly useful for password recovery because they contain usernames and passwords for programs, email, and Internet sites. For recovering login passwords, see "Accessing the SAM File and the System file" on page 129.

RECOVERING PASSWORDS FROM THE CURRENT REGISTRY

PRTK and DNA can retrieve passwords other than Windows user passwords for the following from the current machine's live Windows registry:

- Internet Explorer Content Advisor
- Windows 9x/Me Screen Saver

To recover the password, export the System file to a machine running PRTK or DNA.

PRTK and DNA do not recover screen saver passwords on Windows 2000 or XP systems. However, you can recover screen saver passwords on these systems using the SAM file and System file attack, because the screen saver password is the same as the user's login password. For more information, see "Accessing the SAM File and the System file" on page 129.

RECOVERING PASSWORDS FROM THE REGISTRY PROTECTED STORAGE AREA

PRTK and DNA can recover the following from the protected storage area on the registry:

- Outlook and Outlook Express passwords
- Internet Explorer text fields, such as passwords, emails, and user names submitted online in text fields

The following table identifies the registry files required to recover these passwords on each operating system:

TABLE 9-1 Required Registry Files According to Operating System

Operating System	File
Windows NT/2000/XP	[*drive*]:\Documents and Settings\user\ntuser.dat
Windows 9.*x* system with one configured user	[*drive*]:\Windows_directory\ System
Windows 9.*x* systems with multiple configured users	[*drive*]:\Windows_directory\Profiles\ user\user.dat

Unfortunately, Windows locks these registry files; therefore, they cannot be directly accessed through the operating system.

To access these files, you must do one of the following:

- If you are using FTK Imager, export the file.

  FTK Imager bypasses the Windows operating system, allowing you to copy the file underneath the Windows file lock. The only potential problem is that if the file is being written to during the copy operation, you might get a corrupted copy.
- If you have an image, extract the file from the file directory.

If you are not using FTK Imager or if you do not have an image, boot your computer from a boot disk and copy the file from the system drive.

To boot your computer from a boot disk and copy the ntuser.dat or user.dat file:

1. Restart the computer with a boot disk that is able to read your system drive.

   If the system drive is a FAT partition, you can use a Windows 98 boot disk. If the system drive is an NTFS partition, you must use a Linux or NTFSDOS boot disk.
2. After booting to the boot disk, go to the associated file directory.
3. Copy the file to another location, such as a thumb drive or a network directory.
4. Restart the computer normally.

After you obtain the ntuser.dat, System, or user.dat file, you can perform the password recovery as follows:

1. Start the recovery job. In PRTK or DNA, select *File* > *Add Files* and then select the file, or drag and drop the file into the PRTK or DNA Window.
2. Specify the module options.
3. Select the profile to use.

PRTK and DNA analyze the file and recover the Outlook or Outlook Express password and the Internet Explorer text fields.

RECOVERING AOL COMMUNICATOR ACCOUNT PASSWORDS

AOL Communicator Account Passwords are encrypted in .pref files. The keys needed to decrypt the .pref files are contained in the keyS.db file, which is protected by the master password. To recover these passwords, PRTK and DNA do a dictionary attack on the keyS.db file. After the master password is recovered, the .pref files can be decrypted.

To recover an AOL Communicator Account Password, first recover the master password from keyS.db in [drive]:\Documents and Settings\username\Application

Data\NSS PKI Store\AOL; then recover the .pref files in [*drive*]:\Documents and Settings\username\Application Data\AOL Communicator.

Recovering AOL Instant Messenger Passwords

AOL Instant Messenger Passwords are stored in the storage area of the registry, located in the user's ntuser.dat file.

To recover an AOL Instant Messenger Password:

1. Obtain the user's ntuser.dat file.

   To access the protected storage area of the registry, see "Recovering Passwords from the Registry Protected Storage Area" on page 136.
2. Add the ntuser.dat file to the PRTK or DNA job queue.

Recovering AOL Sign-on Passwords

For AOL versions 8.0 and 9.0, sign-on passwords (including guest logins) are encrypted in the main.idx file ([drive]:\Documents and Settings\All Users\Application Data\AOL\C_America Online version\idb\main.idx).

For AOL 9.0 Security Edition, sign-on passwords are encrypted in SNMaster.idx ([drive]:\Documents and Settings\All Users\ Application Data\AOL\ C_America Online version\ idb\SNMaster.idx).

To recover an AOL Sign-on Password, you need the volume serial number of the C: drive. If there is no C: drive, AOL does not use the volume serial number and PRTK and DNA can immediately recover the sign-on passwords.

- If you are running PRTK or DNA on the original computer, the serial number is automatically found.
- If you are using FTK Imager, you can find the serial number in the Properties window. Once you know the volume serial number, enter it in the Module Options dialog in PRTK or DNA.
- If no volume serial number is supplied, PRTK or DNA begins a keyspace attack.

Recovering MSN Messenger Login Passwords

MSN Messenger Login passwords are recovered differently, depending on the Windows operating system.

Note: To recover an MSN Messenger Login password, the user must have selected the Remember Password option for the system to store this information.

WINDOWS 95/98/ME

On Windows 95/98/Me systems, the password is obscured in the registry.

Important: PRTK and DNA do not run on Windows 9.*x* systems. Therefore, you cannot recover these passwords in their native environment. You must copy them to a Windows 2000, XP, or Vista system.

To recover an MSN Messenger Login password:

1. Obtain the user's ntuser.dat file.

   To access the protected storage area of the registry, see "Recovering Passwords from the Registry Protected Storage Area" on page 136.
2. Copy the file to a machine running PRTK or DNA.
3. Add the ntuser.dat file to the job queue.

WINDOWS 2000

On Windows 2000 systems, the password is encrypted in the registry. Before the password can be decrypted, the EFS master key files must be cracked.

To recover an MSN Messenger Login Password:

1. Recover the Windows login password from the SAM file and System file.
2. Copy the EFS master key files from [drive]:\Documents and Settings\username\Application Data\Microsoft\Protect\ user_SID.
3. Add the ntuser.dat file to the job queue.

Note: When using FTK 2.x in conjunction with PRTK or DNA, you must export the EFS master key file, along with any other EFS-related keys from the FTK case and add them as jobs in either PRTK or DNA. PRTK or DNA then performs an EFS attack to obtain the login password. Since FTK2.x and either PRTK or DNA should not be installed on the same machine, exporting the files and moving them to the PRTK or DNA Supervisor machine is the only way to accomplish EFS file decryption.

Further, when running FTK 1.x, there is an option to do an Advanced EFS attack. Use this option with either PRTK or DNA installed on the same machine with FTK 1.x, and FTK will transfer the files to PRTK or DNA automatically. The FTK and the PRTK or DNA programs must use the same dongle on the same machine to support this integrated functionality.

WINDOWS XP

On Windows XP systems, the password is encrypted in the user's credential file. The credential file cannot be decrypted until the EFS master key files are cracked.

To recover an MSN Messenger Login Password:

1. Recover the Windows login password from the SAM file and System file.
2. Copy the EFS master key files from [*drive*]:\Documents and Settings\username\Application Data\Microsoft\Protect\ user_SID.
3. Perform the password recovery on the credential file in [drive]:\Documents and Settings\[username]\Application Data\Microsoft\Credentials\[user_SID]\Credentials.

   Note: When used in conjunction with PRTK or DNA, FTK sends PRTK or DNA the EFS master key file, along with any other EFS-related keys. The EFS attack is then performed to obtain the login password. FTK and PRTK or DNA must be running on the same dongle on the same machine to support this integrated functionality.

RECOVERING NETSCAPE .W AND .S FILES

Netscape .W and .S files store sensitive user information such as credit card numbers and website passwords. They are encrypted with a key stored in the key3.db file in the same directory ([drive]:\Documents and Settings\[username]\Application Data\Mozilla\Profiles\default\directory.slt\).

To recover Netscape .W and .S files, first recover the master password from key3.db, then recover the Netscape .W and .S files.

RECOVERING QUICKBOOKS PASSWORDS

PRTK and DNA reset the file passwords for QuickBooks 2003 or later. To open a recovered file, open it in QuickBooks and enter a blank password when prompted.

PRTK and DNA use a decryption attack to recover the file passwords for QuickBooks 2002 or earlier. To open a recovered file, open it in QuickBooks and enter the recovered password when prompted.

RECOVERING YAHOO! MESSENGER LOGIN PASSWORDS

Yahoo! Messenger Login Passwords are stored in the protected storage area of the registry located in the user's ntuser.dat file.

To recover a Yahoo! Messenger Login Password:

1. Obtain the user's ntuser.dat file.

   To access the protected storage area of the registry, see "Recovering Passwords from the Registry Protected Storage Area" on page 136.

2. Perform the password recovery.

   Note: You can use FTK to recover Yahoo! Messenger chat logs.

RECOVERING WINZIP ARCHIVE FILES

WinZip versions 6.0 through 8.1 have a security flaw in their encryption algorithm. By using a divide-and-conquer attack called the "WinZip Superfast Attack," AccessData is able to exploit this flaw to recover files from archives created with these versions of WinZip.

Note: WinZip 9.0 files are encrypted with the AES (Advanced Encryption Standard) algorithm and therefore cannot be recovered using the WinZip Superfast Attack.

The WinZip Superfast Attack is not a standard key space attack. It breaks the key space down much more quickly than a linear key space because it intelligently narrows down the zip keys, effectively processing a trillion keys per second.

After the WinZip Superfast Attack recovers the zip keys, it attempts to recover the original password by performing a dictionary attack of passwords up to seven characters.

If Decrypt file when key is found is marked in the Preferences dialog, PRTK and DNA decrypt the file using the zip key. The program then saves the file as [filename]Recovered.zip in the directory designated in the Preferences dialog. The recovered file can be opened without a password. However, if the files contained in the.zip file are passworded or otherwise encrypted, they must be added to PRTK or DNA as additional, separate jobs. For more information on configuring the PRTK or DNA decryption options, see "Specifying Recovery Preferences" on page 77.

RECOVERING IE7 PROTECTEDREGISTRY (INTELLIFORMS) FILES

While PRTK and DNA have a module that addresses Windows Internet Explorer (IE)7 Protected Registry files, there is a specific way to go about collecting and adding these files as jobs.

If you have questions about the different components of this recovery, see "Component Details" on page 144.

COLLECTING NECESSARY IE7 FILES

Before you attempt to follow the steps outlined below you will want to have the following items available in the same place.

It is recommended that you export these items from an image or a live system running Internet Explorer 7:

To begin, create a special folder and export the following files from an FTK case:

ANALYSIS OF A WINDOWS 2000/XP/SERVER 2003 SYSTEM

1. Master Key File: Export

   [*Drive*]:\Documents and Settings\[username]\Application Data\Microsoft\Protect

   in such a way that the contents of the Protect folder will be available in their entirety.
2. Registry files for the system

   Export all of the following:

   - [*Drive*]\Windows\System32\config\SAM
   - [*Drive*]\Windows\System32\config\System
   - [*Drive*]\Documents and Settings\[Username]\NTuser.dat
3. IE Browsing history: Export

   [*Drive*]\Documents and Settings\[Username]\Local Settings\History\History.IE5\index.dat
4. Protect folder: Run a recursive export from:

   [*Drive*]\Documents and Settings\[Username]\Roaming\Microsoft\Protect

   folder.
5. IE7 Internet Browsing History of URLs Index.dat
6. Find the file in

   [*Drive*]\Documents and Settings\[username]\Local Settings\Microsoft\Windows\History\Low\
7. Output.txt – Choose a location for, and create a blank output text file by this name.

ANALYSIS OF A WINDOW VISTA SYSTEM

1. Master Key File: Export

   [*Drive*]:\Users\[UserName]\AppData\Roaming\Microsoft\Protect

   in such a way that the contents of the Protect folder will be available in their entirety)
2. Vista Registry Hives
   - [*Drive*]:\Windows\System32\config\SAM
   - [*Drive*:]\Windows\System32\config\SYSTEM
   - [*Drive*]:\Users\%Username%\NTuser.dat
3. Vista Index.dat file:
   - *Drive*]:\Users\[Username]\AppData\Local\Microsoft \Windows\History\Low\History.IE5\index.dat

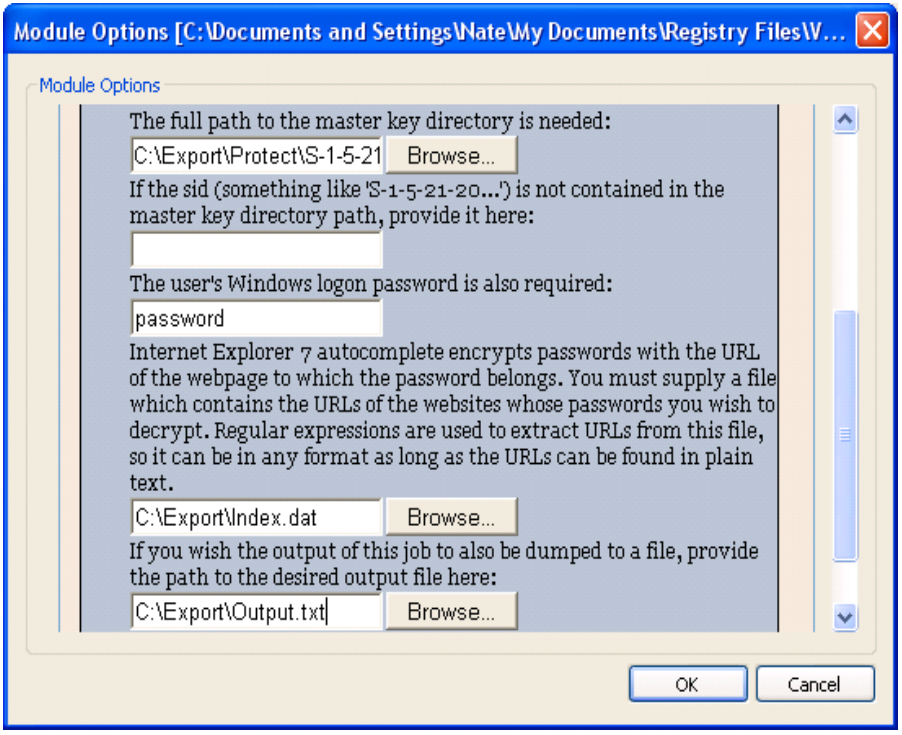
STEPS TO COMPLETE

Use the following steps to use PRTK or DNA to decrypt data protected by DPAPI:

1. Drop the NTUSER.dat into PRTK/DNA.
2. When the attack module is identified, it should recognize that the protected storage section is from IE7 and should prompt you for the:
   - The Windows login password (If you do not know the user's password you will need to recover the password using the SAM and SYSTEM registry files exported in "Collecting Necessary IE7 Files" on page 142 (For more information see "Recovering Login Passwords on Windows 2000 and XP Systems" on page 133).

   In the case that the user's password is blank, you can just leave the password field blank.
   - The folder named with the user's SID that contains the master key files.
   - The index.dat from the browsing history.
   - Output file: If no path is provided, the file will be saved to %SystemRoot%\Program Files\AccessData\PRTK 6 or DNA 3

3. With all the fields completed out correctly (see below screen shot) PRTK/DNA should be able to display the protected data stored for each URL provided when you examine the defined output file.


Module Options [C:\Documents and Settings\Nate\My Documents\Registry Files\V...
Module Options
The full path to the master key directory is needed:
C:\Export\Protect\S-1-5-21
Browse...
If the sid (something like 'S-1-5-21-20...') is not contained in the master key directory path, provide it here:
The user's Windows logon password is also required:
password
Internet Explorer 7 autocomplete encrypts passwords with the URL of the webpage to which the password belongs. You must supply a file which contains the URLs of the websites whose passwords you wish to decrypt. Regular expressions are used to extract URLs from this file, so it can be in any format as long as the URLs can be found in plain text.
C:\Export\Index.dat
Browse...
If you wish the output of this job to also be dumped to a file, provide the path to the desired output file here:
C:\Export\Output.txt
Browse...
OK
Cancel

The above screen shot assumes you exported the files mentioned in "Collecting Necessary IE7 Files" on page 142, to C:\Export\. This serves as an example of what you would see if you correctly fill in the fields of the IE7 Autocomplete Data decryption module.

4. When all fields are populated, click *OK*.

COMPONENT DETAILS

If you have questions about the items referenced above, this section gives an explanation of each.

IE 7

Since IE 7 auto-complete data is encrypted with the Data Protection API, the user must supply the module with the corresponding windows password, Master key file, and SID.

The auto-complete data also has another layer of protection: each piece of data is additionally encrypted with its corresponding URL string. This means that the user must also supply the module with a file that contains the URLs of each piece of auto-complete data. The module uses regular expressions to find URLs in this file, so it doesn't need to have any particular format. A very good choice for this file is the index.dat file, since it usually contains the user's IE browsing history:

```
%SystemRoot%\Documents and Settings\%Username% \Local Settings\History\
History.IE5\index.dat
```

DATA PROTECTION API

To help further protect sensitive information from unauthorized access and tampering, Windows has also implemented an operating system level protection protocol. The more robust cryptographic system, called the Data Protection Application Programming Interface (DPAPI), employs the use of a Triple-DES/CBC algorithm, and a pair of CryptoAPI calls, "CryptoProtectData" and "CryptoUnprotectData," in conjunction with a host application, such as Internet Explorer v7, to encrypt/decrypt session data. The output of the algorithm is a 512-bit master key, based upon a SHA-1 of the user's Windows logon credentials (SHA-1 hash of logon password), as well as 16 random bytes of user data.

To further secure the key, the algorithm also cycles 4,000 times before producing the fixed-length output of the master key. The master key is stored in the user's Protect folder, in a subdirectory labeled with the user SID. A symmetrical session key is generated from the master key. The session key is not stored, only the 16 bytes of random data used in conjunction with the master key to generate it.

The final layer of security within the DPAPI is a 90-day expiration for the master key. After 3 months, a new master key is generated, using the same process, from the user's Windows logon credentials.

An application, such as Internet Explorer v7, calls upon the CryptProtectData function to encrypt session data, such as logon passwords for web sites, search engine queries, or Outlook/Outlook Express account passwords. The encrypted data is stored within the Windows registry, memory, or the file system.

In the registry, encrypted data is stored in the Intelliforms key, and is further maintained within two additional sub-keys, Storage1 and Storage2. The Storage1 key contains form data (auto-complete) and search engine queries, while Storage2 maintains account names and logon passwords.

To access that data, Internet Explorer, or another capable application, calls upon the CryptUnprotectData function, which creates a recovery key, from the master key, to seamlessly decrypt the stored data. The encryption/decryption processes must be performed while either the owner of the encrypted data is logged in, or by accessing the collective components used in the encryption process. As a result, the DPAPI protects sensitive data while the computer is turned off, and from other users who are logged into the same computer.

MASTER KEY FILE

The Windows Data Protection API (DPAPI) uses files called Master Key files (also known as Protect files) to derive session keys for encrypting sensitive data. This is why these files are needed to decrypt data that was encrypted with the Data Protection API.

- The Master Key files corresponding to a user are usually found in the following directory:

  %SystemRoot%\Documents and Settings\{user name}\Application Data\Microsoft\Protect\S-1-5-21-

- The Master Key files themselves have names that look like:

  f1cc77ef-ef76-4c89-8385-20b9a921d2c6

- By default Windows marks these as hidden system files which means that you cannot see them unless you specifically enable Windows Explorer to show those types of files.

SID

Windows assigns a Security ID to each user in a system or domain.

- This ID looks something like this:
  S-1-5-21-560424602-2976196664-1938093919-1006
  (The actual numbers will of course vary from user to user.)
- The SID is used in the Data Protection API as salt in the encryption of the Master key files with the Windows login password. That is why the SID is needed to decrypt data that has been encrypted with the Data Protection API.
- The name of the folder that contains the Master key files is usually the SID.

Chapter 10 Managing Security Devices and Licenses

This chapter acquaints you with the managing AccessData product licenses. Here you will find details regarding the LicenseManager interface and how to manage licenses and update products using LicenseManager.

NLS SUPPORT

In this PRTK 6.5 and DNA 3.5 release, AccessData's Network License Service (NLS) is supported. If you have NLS, you should also have documentation on how to install and implement it.

VIRTUAL CMSTICK

Beginning with the PRTK 6.5 and DNA 3.5 release, AccessData's new Virtual CmStick is supported. The Virtual CmStick is a file that allows full use of the program without worry that the USB CmStick could be lost or stolen. Licenses can be bound and un-bound to the Virtual CmStick just as with the USB CmStick, however, the Virtual CmStick is not transferable from one machine to another. (15228)

Talk to your Sales Representative about purchasing this option.

INSTALLING AND MANAGING SECURITY DEVICES

Before you can manage licenses with LicenseManager, you must install the proper security device software and/or drivers. This section explains installing and using the Wibu CodeMeter Runtime software and USB CmStick, as well as the Keylok USB dongle drivers and dongle device.

INSTALLING THE SECURITY DEVICE

As discussed previously, AccessData products require a licensing security device that communicates with the program to verify the existence of a current license. The device can be the older Keylok dongle, or the newer Wibu CmStick. Both are USB devices, and both require specific software to be installed prior to connecting the devices and running your AccessData products. You will need:

- The Wibu CodeMeter Runtime software with a Wibu CodeMeter (CmStick)
- The Wibu CodeMeter Runtime software, and the AccessData Dongle Drivers with a Keylok dongle

Note: The Codemeter Runtime software and either a silver Wibu CmStick or a green Keylok dongle are required to run PRTK or DNA. Without them, you can run PRTK or DNA in Demo mode only.

The CmStick or dongle should be stored in a secure location when not in use.

You can install PRTK and the CodeMeter software from the shipping CD or from downloadable files available on the AccessData website at www.accessdata.com. Click *Support* > *Downloads*, and browse to the product to download. Click the download link and save the file locally prior to running the installation files.

For solutions to commonly asked installation questions, see "Chapter 11 Troubleshooting" on page 173.

INSTALLING THE CODEMETER RUNTIME SOFTWARE

When you purchase the full PRTK package, AccessData provides a USB CmStick with the product package. The green Keylok dongles are no longer provided, but can be purchased separately through your AccessData Sales Representative.

To use the CmStick, you must first install the CodeMeter Runtime software, either from the shipping CD, or from the setup file downloaded from the AccessData Web site.

LOCATING THE SETUP FILE

To install the CodeMeter Runtime software from the CD, you can browse to the setup file, or select it from the Autorun menu.

To download the CodeMeter Runtime software, go to www.accessdata.com and do the following:

1. Click *Support* > *Downloads*.

2. Find CodeMeter Runtime 4.10c (32-bit)

   MD5: 7cc6506452af3761fd306c4249a3223e

   (MD5 hash applies only to this version)

   OR

   Find CodeMeter Runtime 4.10c (64-bit)

   MD5: fa7a268bbbf4db75cdc52333ca663d11

   (MD5 hash applies only to this version)

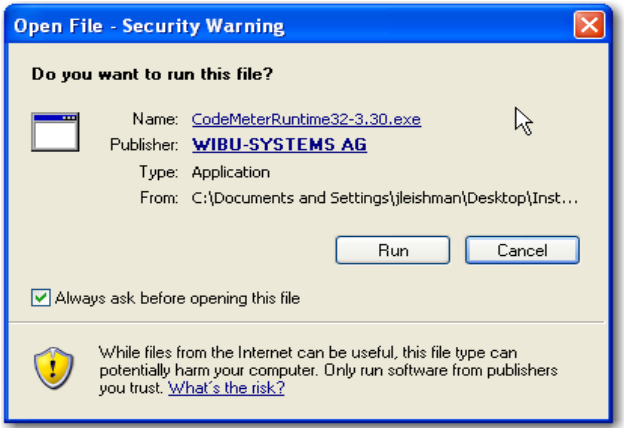
3. Click the *Download* link.
4. Save the file to your PC and run after the download is complete.

When the download is complete, double-click on the CodeMeterRuntime32-3.30.exe.

RUNNING THE CODEMETER RUNTIME SETUP

Whichever way you choose to access the CodeMeter Runtime setup file, when you run it you will see the following:

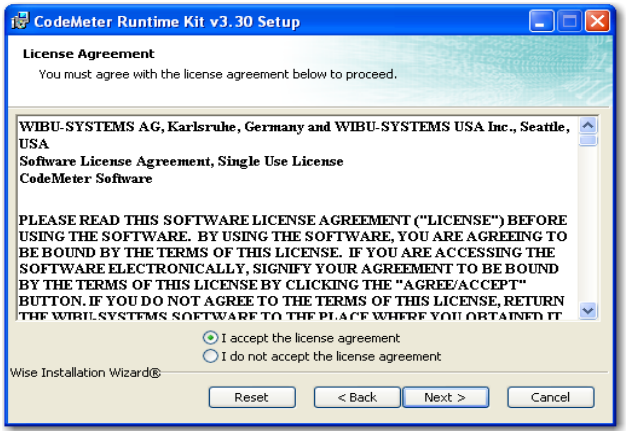
1. The CodeMeter Runtime Open File Security Warning will appear to allow you to verify that you really want to open this file.


Open File - Security Warning
Do you want to run this file?
Name: CodeMeterRuntime32-3.30.exe
Publisher: WIBU-SYSTEMS AG
Type: Application
From: C:\Documents and Settings\jleishman\Desktop\Inst...
Run
Cancel
Always ask before opening this file
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

2. Click *Run*.

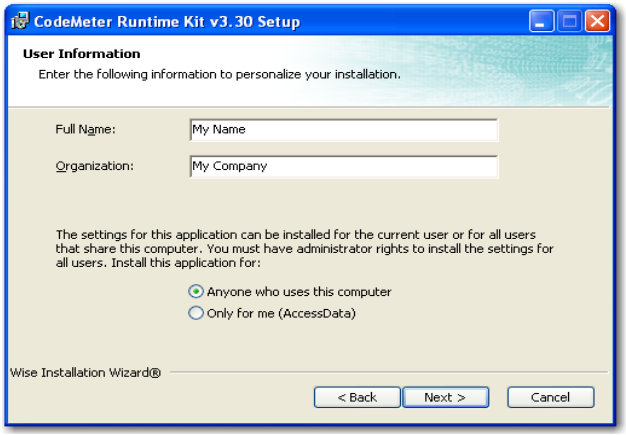
CodeMeter Runtime Kit v3.30 Setup
Welcome to the CodeMeter Runtime Kit v3.30 Installation Wizard
It is strongly recommended that you exit all Windows programs before running this setup program.
Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
< Back
Next >
Cancel

3. On the Welcome screen, click *Next*.

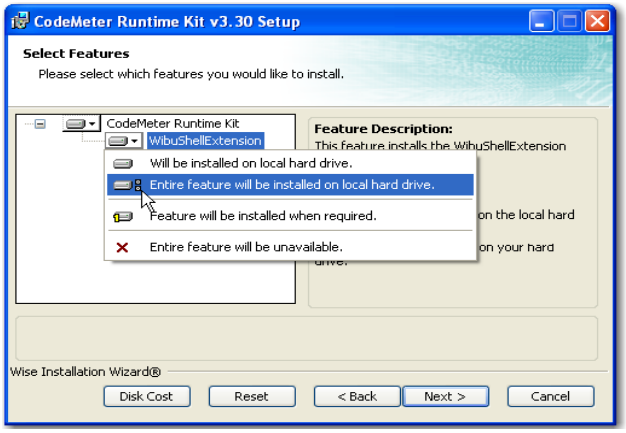

CodeMeter Runtime Kit v3.30 Setup
License Agreement
You must agree with the license agreement below to proceed.
WIBU-SYSTEMS AG, Karlsruhe, Germany and WIBU-SYSTEMS USA Inc., Seattle, USA
Software License Agreement, Single Use License
CodeMeter Software
PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") BEFORE USING THE SOFTWARE. BY USING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU ARE ACCESSING THE SOFTWARE ELECTRONICALLY, SIGNIFY YOUR AGREEMENT TO BE BOUND BY THE TERMS OF THIS LICENSE BY CLICKING THE "AGREE/ACCEPT" BUTTON. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, RETURN
I accept the license agreement
I do not accept the license agreement
Wise Installation Wizard®
Reset
< Back
Next >
Cancel

4. Accept the License Agreement.

5. Click *Next*.

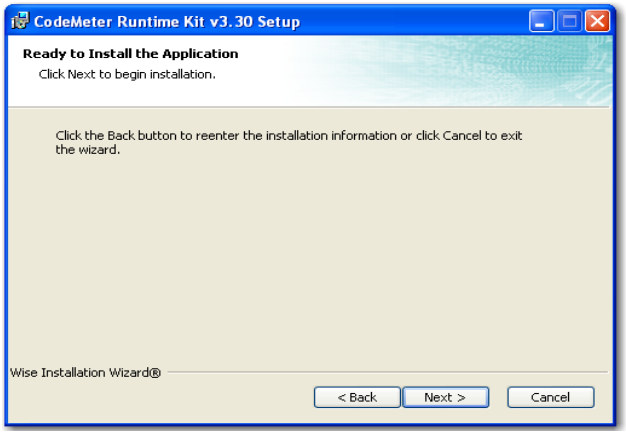

CodeMeter Runtime Kit v3.30 Setup
User Information
Enter the following information to personalize your installation.
Full Name:
My Name
Organization:
My Company
The settings for this application can be installed for the current user or for all users that share this computer. You must have administrator rights to install the settings for all users. Install this application for:
Anyone who uses this computer
Only for me (AccessData)
Wise Installation Wizard®
< Back
Next >
Cancel

6. In the User Information screen, enter your name and your company name.
7. Specify whether this application should be available only when you log in, or for anyone who uses this computer.
8. Click *Next*.


CodeMeter Runtime Kit v3.30 Setup
Select Features
Please select which features you would like to install.
CodeMeter Runtime Kit
WibuShellExtension
Will be installed on local hard drive.
Entire feature will be installed on local hard drive.
Feature will be installed when required.
Entire feature will be unavailable.
Feature Description:
This feature installs the WibuShellExtension
Wise Installation Wizard®
Disk Cost
Reset
< Back
Next >
Cancel

9. Select the features you want to install.

10. Click *Next*.


CodeMeter Runtime Kit v3.30 Setup
Ready to Install the Application
Click Next to begin installation.
Click the Back button to reenter the installation information or click Cancel to exit the wizard.
Wise Installation Wizard®
< Back
Next >
Cancel

11. When you are satisfied with the options you have selected, click *Next*.

CodeMeter Runtime Kit v3.30 Setup
CodeMeter Runtime Kit v3.30 has been successfully installed.
Click the Finish button to exit this installation.
< Back
Finish
Cancel

12. Installation will run its course. When complete, you will see the "CodeMeter Runtime Kit v3.30 has been successfully installed" screen. Click *Finish* to exit the installation.

THE CODEMETER CONTROL CENTER

When the CodeMeter Runtime installation is complete, the CodeMeter Control Center pops up. This is a great time to connect the CmStick and verify that the device is recognized and is Enabled. Once verified, you can close the control center and run your AccessData product(s).

For the most part there is nothing you need to do with this control center, and you need make no changes using this tool with very few exceptions. If you have problems

with your CmStick, contact AccessData Support and an agent will walk you through any troubleshooting steps that may need to be performed.

INSTALLING KEYLOK DONGLE DRIVERS

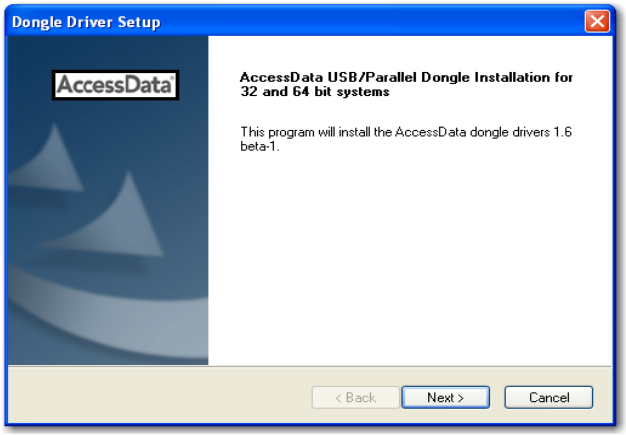
To install the Keylok USB dongle drivers do the following:

1. If installing from CD, insert the CD into the CD-ROM drive and click *Install the Dongle Drivers*.

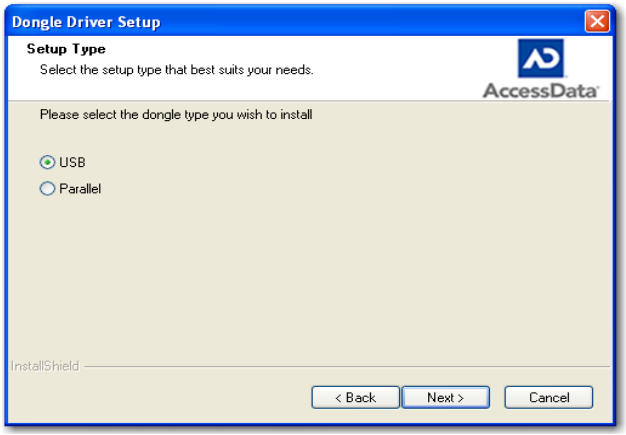
   If auto-run is not enabled, select *Start* > *Run*. Browse to the CD-ROM drive and select Autorun.exe.

   OR

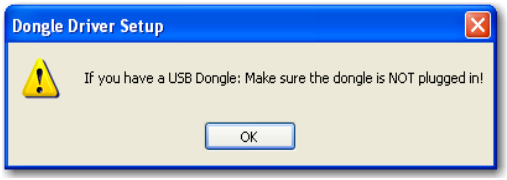
1. If installing from a file downloaded from the AccessData Web site, locate the Dongle_driver_1.6.exe setup file, and double-click it.


Dongle Driver Setup
AccessData
AccessData USB/Parallel Dongle Installation for 32 and 64 bit systems
This program will install the AccessData dongle drivers 1.6 beta-1.
< Back
Next >
Cancel

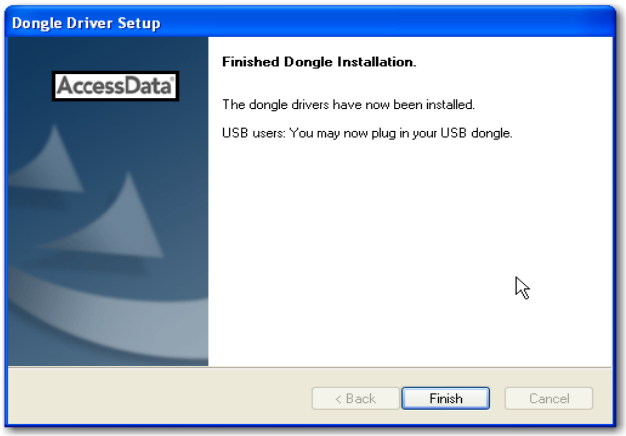
2. Click *Next*.



3. Select the type of dongle to install the drivers for.
4. Click *Next*.



5. If you have a USB dongle, verify that it is not connected.
6. Click *Next*.



7. Click *Finish*.
8. Connect the USB dongle. Wait for the Windows Found New Hardware wizard, and follow the prompts.

Important: If the Windows Found New Hardware wizard appears, complete the wizard. Do not close without completing, or the dongle driver will not be installed.

Windows Found New Hardware Wizard

When you connect the dongle after installing the dongle drivers, you should wait for the Windows Found New Hardware Wizard to come up. It is not uncommon for users to disregard this wizard, and then find that the dongle is not recognized and their AccessData software will not run.

When the Found New Hardware Wizard pops up, do the following:

1. When prompted whether to connect to Windows Update to search for software, choose, “No, not this time”.

Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).
Read our privacy policy
Can Windows connect to Windows Update to search for software?
Yes, this time only
Yes, now and every time I connect a device
No, not this time
Click Next to continue.
< Back
Next >
Cancel

2. Click *Next*.
3. When prompted whether to install the software automatically or to install from a list of specific locations, choose, “Install the software automatically (Recommended)”.

Found New Hardware Wizard
This wizard helps you install software for:
USB Dongle - Software Protection Device
If your hardware came with an installation CD or floppy disk, insert it now.
What do you want the wizard to do?
Install the software automatically (Recommended)
Install from a list or specific location (Advanced)
Click Next to continue.
< Back
Next >
Cancel

4. Click *Next*.

5. Click *Finish* to close the wizard.

Found New Hardware Wizard
Completing the Found New Hardware Wizard
The wizard has finished installing the software for:
USB Dongle - Software Protection Device
Click Finish to close the wizard.
< Back
Finish
Cancel

Once you have installed the dongle drivers and connected the dongle and verified that Windows recognizes it, you can use LicenseManager to manage product licenses.

INSTALLING LICENSEMANAGER

LicenseManager lets you manage product and license subscriptions using a security device or device packet file. For more information, see "Chapter 10 Managing Security Devices and Licenses" on page 147.

Note: You can install LicenseManager from the PRTK or DNA installation disc, or the installation files are available on the AccessData Website.

To install LicenseManager from the downloadable file:

1. Go to the AccessData download page at http://www.accessdata.com/downloads.htm.
2. On the download page, click the *LicenseManager Download* link.
3. Save the installation file (currently lm-license_manager-2.2.4.exe) to a temporary directory on your drive.
4. To launch the installation program, go to the temporary directory and double-click the installation file you downloaded in step 3.

5. Click *Next* on the Welcome screen.

AccessData Password Recovery Toolkit - InstallShield Wizard
AccessData
Password Recovery Toolkit
The InstallShield Wizard will install AccessData Password Recovery Toolkit on your computer. To continue, click Next.
< Back
Next >
Cancel

6. Click *Yes* to accept the license agreement.

AccessData Password Recovery Toolkit - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
AccessData
AccessData® Corp. End User License Agreement
THIS IS A LEGAL AGREEMENT between "you," the end user of AccessData Corp. brand software, and AccessData Corp. (AccessData).
Use of the software you have downloaded or are about to install indicates your acceptance of these terms. As used in this Agreement, the capitalized term "Software" means the AccessData® software together with any and all enhancements, upgrades, and updates that may be provided to you in the future by AccessData. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, YOU SHOULD SO INDICATE AT THE APPROPRIATE SCREEN AND PROMPTLY DISCONTINUE THE INSTALLATION AND DOWNLOAD PROCESS.
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
InstallShield
< Back
Next >
Cancel

7. Wait while the installation completes.

8. If you want to launch LicenseManager after completing the installation, select *Run LicenseManager*.

Run LicenseManager later by selecting
Start >*Programs* > *AccessData* > *LicenseManager* > *LicenseManager*
or by double-clicking the LicenseManager icon on your desktop .

MANAGING LICENSES WITH LICENSEMANAGER

LicenseManager manages AccessData product licenses on a Keylok dongle or Wibu CodeMeter Stick security device, or in a security device packet file. LicenseManager and the CodeMeter Stick installation are no longer integrated with FTK2 installation.

LicenseManager displays license information, allows you to add or remove existing licenses to a dongle or CmStick. LicenseManager can also be used to export a security device packet file. Packet files can be saved and reloaded onto the dongle or CmStick, or sent via email to AccessData support.

In addition, you can use LicenseManager to check for product updates and download the latest product versions.

LicenseManager displays CodeMeter Stick information (including packet version and serial number) and licensing information for all AccessData products. The Purchase Licenses button connects directly to the AccessData website and allows you to browse the site for information about products you may wish to purchase. Contact AccessData by phone to speak with a Sales Representative for answers to product questions, and to purchase products and renew licenses and subscriptions.

LicenseManager provides information as displayed in the following figures:

Figure 10-1 LicenseManager Installed Components Tab

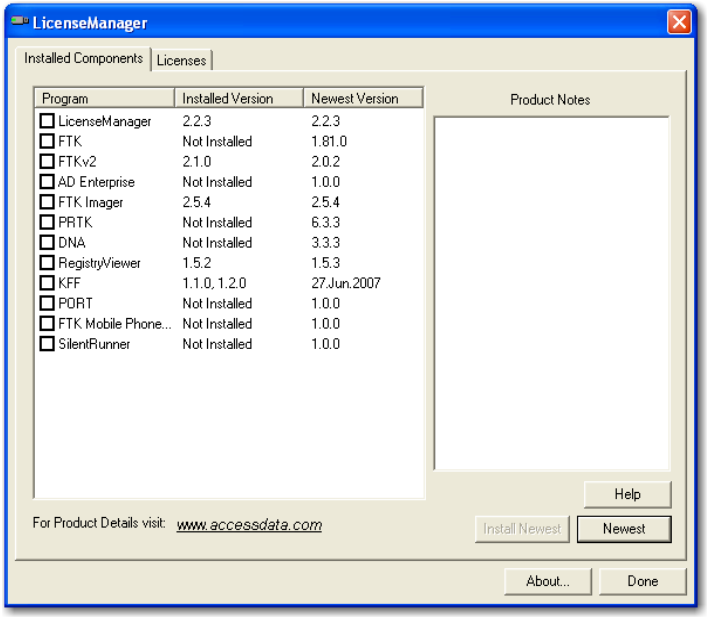
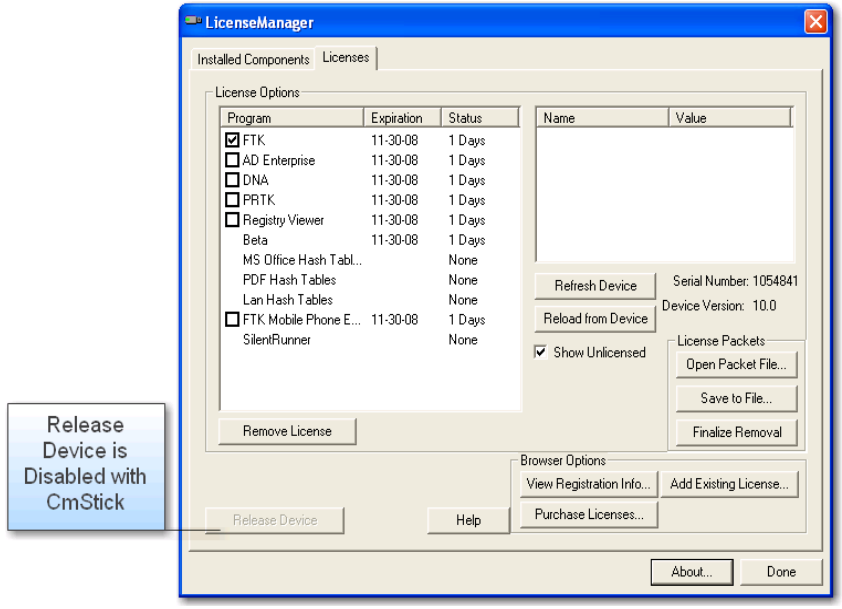


Figure 10-2 LicenseManager Licenses Tab



STARTING LICENSEMANAGER

LicenseManager.exe is located in C:\Program Files\AccessData\Common Files\AccessData LicenseManager\. You can execute the program from this location if you wish.

Click *Start* > *All Programs* > *AccessData* > *LicenseManager* > *LicenseManager,*

OR

Click or double-click (depending on your Windows settings) the *LicenseManager* icon on your desktop .

OR

From some AccessData programs, you can run LicenseManager from the *Tools* > *Other Applications* menu. This option is not available in PRTK or DNA.

The LicenseManager program opens.

When starting LicenseManager, License Manager reads licensing and subscription information from the installed and connected Wibu CodeMeter Stick, or Keylok dongle.

If using a Keylok dongle, and LicenseManager either does not open or displays the message, "Device Not Found", do the following:

1. Make sure the correct dongle driver is installed on your computer.
2. With the dongle connected, check in Windows Device Manager to make sure the device is recognized. If it has an error indicator, right click on the device and choose Uninstall.
3. Remove the dongle after the device has been uninstalled.
4. Reboot your computer.
5. After the reboot is complete, and all startup processes have finished running, connect the dongle.
6. Wait for Windows to run the Add New Hardware wizard. If you already have the right dongle drivers installed, do not browse the internet, choose, "No, not this time."
7. Click *Next* to continue.
8. On the next options screen, choose, "Install the software automatically (Recommended)
9. Click Next to continue.
10. When the installation of the dongle device is complete, click Finish to close the wizard.
11. You still need the CodeMeter software installed, but will not need a CodeMeter Stick to run LicenseManager.

If using a CodeMeter Stick, and LicenseManager either does not open or displays the message, "Device Not Found", do the following:

1. Make sure the CodeMeter Runtime 3.30a software is installed. It is available at www.accessdata.com/support. Click Downloads and browse to the product. Click on the download link. You can Run the product from the Website, or Save the file locally and run it from your PC. Once the CodeMeter Runtime software is installed and running, you will see a gray icon in your system tray: .
2. Make sure the CodeMeter Stick is connected to the USB port. When the CmStick is then connected, you will see the icon change to look like this: .

If the CodeMeter Stick is not connected, LicenseManager still lets you to manage licenses using a security device packet file if you have exported and saved the file previously.

To open LicenseManager without a CodeMeter Stick installed:

1. Click *Tools* > *LicenseManager*.

   LicenseManager displays the message, "Device not Found".

2. Click *OK*, then browse for a security device packet file to open.

Note: Although you can run LicenseManager using a packet file, FTK2.1 will not run with a packet file alone. You must have the CmStick connected to the computer to run FTK2.1.

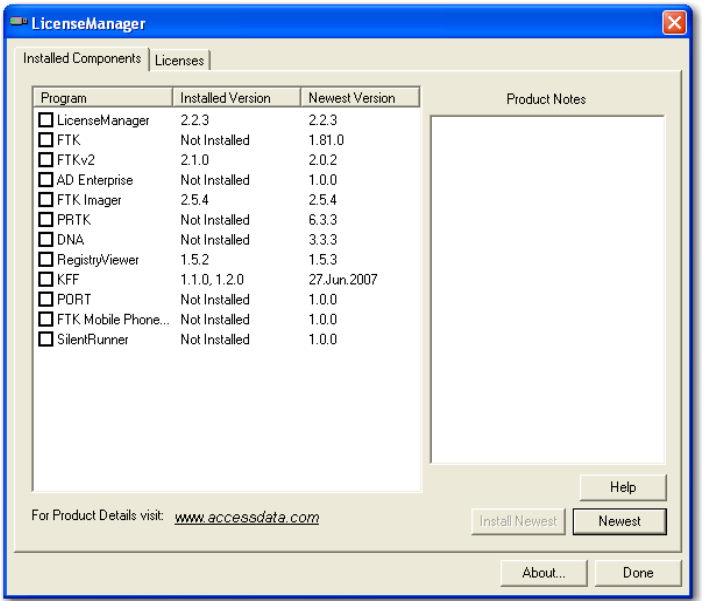
THE LICENSEMANAGER INTERFACE

The LicenseManager interface consists of two tabs that organize the options in the LicenseManager window: the Installed Components tab and the Licenses tab.

THE INSTALLED COMPONENTS TAB

The Installed Components tab lists the AccessData programs installed on the machine. The Installed Components tab is displayed in the following figure.

Figure 10-3 LicenceManager Installed Components



The following information is displayed on the Installed Components tab:

TABLE 10-1 LicenseManager Installed Components Tab Features

Item	Description
Program	Lists all AccessData products installed on the host.
Installed Version	Displays the version of each AccessData product installed on the host.
Newest Version	Displays the latest version available of each AccessData product installed on the host. Click Newest to refresh this list.
Product Notes	Displays notes and information about the product selected in the program list.
AccessData Link	Links to the AccessData product page where you can learn more about AccessData products.

The following buttons provide additional functionality from the Installed Components tab:

TABLE 10-2 LicenseManager Installed Components Buttons

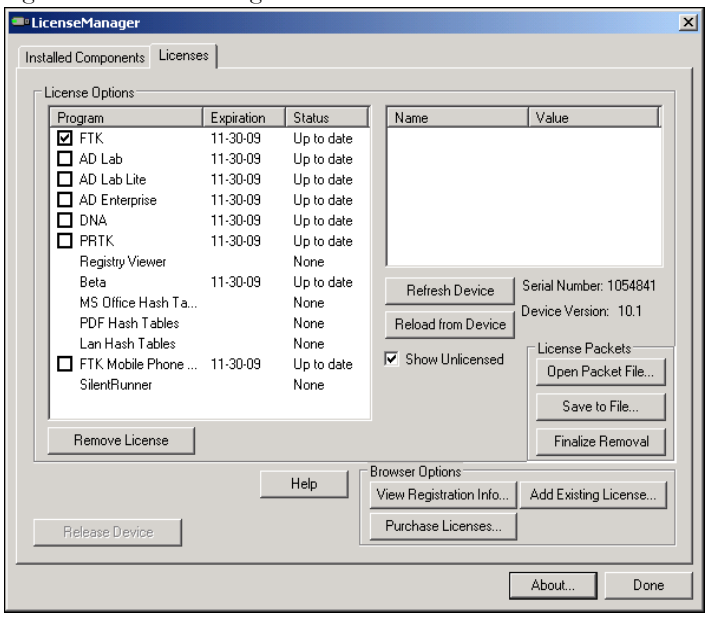
Button	Function
Help	Opens the LicenseManager Help web page.
Install Newest	Installs the newest version of the programs checked in the product window, if that program is available for download. You can also get the latest versions from our website using your Internet browser.
Newest	Updates the latest version information for your installed products.
About	Displays the About LicenseManager screen. Provides version, copyright, and trademark information for LicenseManager.
Done	Closes LicenseManager.

Use the Installed Components tab to manage your AccessData products and stay up to date on new releases.

THE LICENSES TAB

The Licenses tab displays CodeMeter Stick information for the current security device packet file and licensing information for AccessData products available to the owner of the CodeMeter Stick, as displayed in the following figure.

Figure 10-4 LicenseManager Licenses Tab



The Licenses tab provides the following information:

TABLE 10-3 LicenseManager Licenses Tab Features

Column	Description
Program	Shows the owned licenses for AccessData products.
Expiration Date	Shows the date on which your current license expires.
Status	Shows these status of that product's license: • **None**: the product license is not currently owned • **Days Left**: displays when less than 31 days remain on the license. • **Never**: the license is permanently owned. This generally applies to Hash Tables and Portable Office Rainbow Tables.

TABLE 10-3 LicenseManager Licenses Tab Features

Column	Description
Name	Shows the name of additional parameters or information a product requires for its license.
Value	Shows the values of additional parameters or information a product contained in or required for its license.
Show Unlicensed	When checked, the License window displays all products, whether licensed or not.

The following license management actions can be performed using buttons found on the License tab:

TABLE 10-4 License Management Options

Button	Function
Remove License	Removes a selected license from the Licenses window and from the CodeMeter Stick or dongle. Opens the AccessData License Server web page to confirm success.
Refresh Device	Connects to the AccessData License Server. Downloads and overwrites the info on the CodeMeter Stick or dongle with the latest information on the server.
Reload from Device	Begins or restarts the service to read the licenses stored on the CodeMeter Stick or dongle.
Release Device	Click to stop the program reading the dongle attached to your machine, much like Windows' Safely Remove Hardware feature. Click this button before removing a dongle. This option is disabled for the CodeMeter Stick.
Open Packet File	Opens Windows Explorer, allowing you to navigate to a .PKT file containing your license information.
Save to File	Opens Windows Explorer, allowing you to save a .PKT file containing your license information. The default location is My Documents.
Finalize Removal	Finishes the removal of licenses in the unbound state. Licenses must be unbound from the CmStick or dongle before this button takes effect.
View Registration Info	Displays an HTML page with your CodeMeter Stick number and other license information.
Add Existing License	Allows you to bind an existing unbound license to your CodeMeter Stick, through an internet connection to the AccessData License Server.

TABLE 10-4 License Management Options

Button	Function
Purchase License	Brings up the AccessData product page from which you can learn more about AccessData products.
About	Displays the About LicenseManager screen. Provides version, copyright, and trademark information for LicenseManager.
Done	Closes LicenseManager.

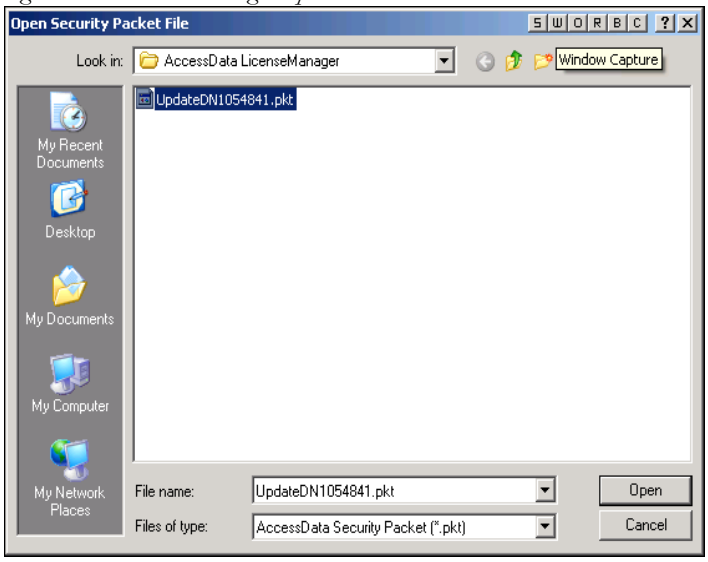
OPENING AND SAVING DONGLE PACKET FILES

You can open or save dongle packet files using LicenseManager. When started, LicenseManager attempts to read licensing and subscription information from the dongle. If you do not have a dongle installed, LicenseManager lets you browse to open a dongle packet file. You must have already created and saved a dongle packet file to be able to browse to and open it.

To open a dongle packet file:

1. Select click the *Licenses* tab, then under License Packets, click *Open Packet File.*
2. Browse for a dongle packet file to open. Select the file, then click *Open.*

Figure 10-5 LicenseManager Open Packet File



To save a dongle packet file:

1. Click the *Licenses* tab, then under License Packets, click *Save to File*.
2. Browse to the desired folder and accept the default name of the .PKT file; then click *Save*.

Note: In general, the best place to save the .PKT files is in the AccessData LicenseManager folder. The default path is C:\Program Files\AccessData\Common Files\AccessData LicenseManager\.

ADDING AND REMOVING PRODUCT LICENSES

On a computer with an Internet connection, LicenseManager lets you add available product licenses to, or remove them from, a dongle.

To move a product license from one dongle to another dongle, first remove the product license from the first dongle. You must release that dongle, and connect the second dongle before continuing. When the second dongle is connected and recognized by Windows and LicenseManager, click on the Licenses tab to add the product license to the second dongle.

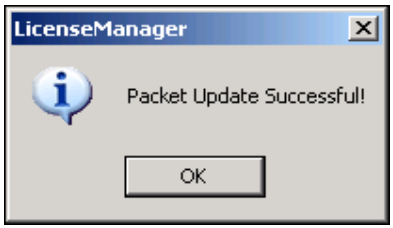
REMOVE A LICENSE

To remove (unbind) a product license:

1. From the Licenses tab, mark the program license to remove. This action activates the Remove License button below the Program list box.
2. Click *Remove License*. This connects your machine to the AccessData License Server through the Internet.
3. You will be prompted to confirm the removal of the selected license(s) from the device. Click *Yes* to continue, or *No* to cancel.

4. You will see some screens indicating the connection and activity on the License Server, and when the license removal is complete, you will see the following screen:

Figure 10-6 Packet Update Successful



5. Click OK to close the message box. You will then see an Internet browser screen from LicenseManager with a message that says, "The removal of your license(s) from Security Device was successful!" You may close this box at any time.

ADD A LICENSE

To add a new or released license:

1. From the Licenses tab, under Browser Options, click *Add Existing License.*

   The AccessData LicenseManager Web page opens, listing the licenses currently bound to the connected security device, and below that list, you will see the licenses that currently are not bound to any security device. Mark the box in the Bind column for the product you wish to add to the connected device, then click *Submit.*

2. An AccessData LicenseManager Web page will open, displaying the following message, "The AccessData product(s) that you selected has been bound to the record for Security Device *nnnnnnn* within the Security Device Database.

   "Please run LicenseManager's "Refresh Device" feature in order to complete the process of binding these product license(s) to this Security Device." You may close this window at any time.

   Click *Yes* if LicenseManager prompts, "Were you able to associate a new product with this device?"

ADDING AND REMOVING PRODUCT LICENSES REMOTELY

While LicenseManager requires an Internet connection to use some features, you can add or remove licenses from a dongle packet file for a dongle that resides on a computer, such as a forensic lab computer, that does not have an Internet connection.

If you cannot connect to the Internet, the easiest way to move licenses from one dongle to another is to physically move the dongle to a computer with an Internet connection, add or remove product licenses as necessary using LicenseManager, and then physically move the dongle back to the original computer. However, if you cannot move the dongle—due to organization policies or a need for forensic soundness—then transfer the packet files and update files remotely.

ADD A LICENSE REMOTELY

To remotely add (bind) a product license:

1. On the computer where the security device resides:
   1a. Run LicenseManager.
   1b. From the *Licenses* tab, click *Reload from Device* to read the dongle license information.
   1c. Click *Save to File* to save the dongle packet file to the local machine.
2. Copy the dongle packet file to a computer with an Internet connection.
3. On the computer with an Internet connection:
   3a. Remove any attached security device.
   3b. Launch LicenseManager. You will see a notification, "No security device found".
   3c. Click *OK*.
   3d. An "Open" dialog box will display. Highlight the .PKT file, and click *Open*.
   3e. Click on the Licenses tab.
   3f. Click *Add Existing License*.
   3g. Complete the process to add a product license on the Website page.
   3h. Click *Yes* when the LicenseManager prompts, "Were you able to associate a new product with this dongle?"
   3i. When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted to save the update file, [serial#].wibuCmRaU.
   3j. Save the update file to the local machine.
4. After the update file is downloaded, copy the update file to the computer where the dongle resides:
5. On the computer where the dongle resides:
   5a. Run the update file by double-clicking it. (It is an executable file.)
   5b. After an update file downloads and installs, click *OK*.

5c. Run LicenseManager.

5d. From the Licenses tab, click *Reload from Device* to verify the product license has been added to the dongle.

REMOVE A LICENSE REMOTELY

To remotely remove (unbind) a product license:

1. On the computer where the dongle resides:
   1a. Run LicenseManager.
   1b. From the Licenses tab, click *Reload from Device* to read the dongle license information.
   1c. Click *Save to File* to save the dongle packet file to the local machine.
2. Copy the file to a computer with an Internet connection.
3. On the computer with an Internet connection:
   3a. Launch LicenseManager. You will see a notification, "No security device found".
   3b. Click *OK*.
   3c. An "Open" dialog box will display. Highlight the .pkt file, and click *Open*.
   3d. Click on the Licenses tab.
   3e. Mark the box for the product license you want to unbind; then click *Remove License*.
   3f. When prompted to confirm the removal of the selected license from the dongle, click *Yes*.

   When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted save the update file.

   3g. Click *Yes* to save the update file to the local computer.

   The Step 1 of 2 dialog details how to use the dongle packet file to remove the license from a dongle on another computer.

   3h. Save the update file to the local machine.
4. After the update file is downloaded, copy the update file to the computer where the dongle resides.
5. On the computer where the dongle resides:
   5a. Run the update file by double-clicking it. This runs the executable update file and copies the new information to the security device.
   5b. Run LicenseManager

5c. On the Licenses tab, click *Reload from Device* in LicenseManager to read the security device and allow you to verify the product license is removed from the dongle.

5d. Click *Save to File* to save the updated dongle packet file to the local machine.

6. Copy the file to a computer with an Internet connection.

UPDATING PRODUCTS

You can use LicenseManager to check for product updates and download the latest product versions.

For more information on the general features of the subscription service, see the AccessData Website at http://www.accessdata.com/subscription_renewal.htm.

CHECK FOR PRODUCT UPDATES

To check for product updates, on the Installed Components tab, click *Newest*. This refreshes the list to display what version you have installed, and the newest version available.

DOWNLOAD PRODUCT UPDATES

To install the newest version, mark the box next to the product to install, then click Install Newest.

Note: Some products, such as FTK 2.x, Enterprise, and others, are too large to download, and are not available. A notification displays if this is the case.

To download a product update:

1. Ensure that LicenseManager displays the latest product information by clicking the Installed Components tab. Click *Newest* to refresh the list showing the latest releases, then compare your installed version to the latest release.

   If the latest release is newer than your installed version, you may be able to install the latest release from our Website.
2. Ensure that the program you want to install is not running.
3. Mark the box next to the program you want to download; then click *Install Newest*.
4. When prompted, click *Yes* to download and install the latest install version of the product.

5. If installing the update on a remote computer, copy the product update file to another computer.
6. Install the product update.

For information about installing the product update, refer to the installation information for the product. You may need to restart your computer after the update is installed.

PURCHASE PRODUCT LICENSES

Use LicenseManager to link to the AccessData Web site to find information about all our products.

Purchase product licenses through your AccessData Sales Representative. Call 801-377-5410 and follow the prompt for Sales, or send an email to sales@accessdata.com.

Note: Once a product has been purchased and appears in the AccessData License Server, add the product license to a CodeMeter Stick, dongle, or security device packet file by clicking *Refresh Device*.

SEND A DONGLE PACKET FILE TO SUPPORT

Send a security device packet file *only* when specifically directed to do so by AccessData support.

To create a dongle packet file, do the following:

1. Run LicenseManager
2. Click on the Licenses tab.
3. Click *Load from Device*.
4. Click *Refresh Device* if you need to get the latest info from AD's license server.
5. Click *Save to File*, and note or specify the location for the saved file.
6. Attach the dongle packet file to an e-mail and send it to: support@accessdata.com.

Chapter 11 Troubleshooting

This chapter explains basic troubleshooting for Password Recovery Toolkit (PRTK) 6.5 and Distributed Network Attack (DNA) 3.5.

PRTK AND DNA TROUBLESHOOTING

The following tables provide problems and suggested solutions for running PRTK or DNA.

INSTALLATION

This section contains solutions to common PRTK installation and upgrade issues and questions.

TABLE 11-1 Installation Troubleshooting

Problem	Possible Cause	Solution
I installed PRTK on a new machine, and my dongle is not working.	Dongle isn't installed properly.	If you do not install the dongle driver correctly, then the product displays "A dongle was not detected. PRTK is now running in DEMO Mode. You will be able to run only jobs with the free modules" message at startup. To make sure you installed the driver correctly, check the following: • Make sure the dongle security hardware is plugged in to the correct port during installation of the dongle driver. • If you do not use the dongle, you cannot access licensed versions of the application modules or use those applications to recover passwords.
How can I download the full version of PRTK from the AccessData Website so that I can use the product immediately?	The full version of PRTK requires a dongle driver for security management.	When you download PRTK from the Web. You cannot use the full version of PRTK until the dongle has been shipped an installed.

PASSWORD RECOVERY

This section contains solutions to the most common PRTK password recovery issues and questions.

TABLE 11-2 Password Recovery Troubleshooting

Problem	Possible Cause	Solution
When I try to recover a password-protected file, PRTK returns the message "Finished. Password not found" What should I do now?		If the recovery failed, then the password could not be located in your custom or default dictionaries. You need to re-evaluate the evidence and create a more detailed custom dictionary. When running a dictionary attack, provide as much information as possible about the person who locked the file. This information can be defined in a biographical dictionary or a custom user dictionary.
I know that my Excel/Word password is made up of all letters or all numbers. Can this information help me recover my password more quickly?		Create a specific profile for this case.
Why can't I recover my Zip file?	Attack needs more time.	The program uses SuperFast Zip Attack if your archive contains five or more files and was created with WinZip 8.0 or an earlier version. This attack generally takes around 2 to 3 hours.
Why don't the Quicken 2002, QuickBooks 2002, WinZip, or VBA files appear in the clipboard after I recover the password?	You did not recover the password for these files; instead, you decrypted the file using the key.	You can access the decrypted version of your file at the location you specified when setting up.
PRTK has been running a dictionary attack for a very long time. Is this normal?		Yes. Double-click the file in PRTK to see the progress. If the number of passwords tested is still increasing, then the recovery is still running.

TABLE 11-2 Password Recovery Troubleshooting

Problem	Possible Cause	Solution
If my computer crashes during a lengthy password recovery, how do I recover the work that was already performed?		Restart the program. PRTK continues the password recovery process for jobs in the session when you restart *PRTK*.

DNA TROUBLESHOOTING

This section contains solutions to the following frequently asked questions.

TABLE 11-3 DNA Troubleshooting FAQs

Problem	Possible Cause	Solution
I cannot add a file to the jobs queue from a different network machine. Why?	Although you might be able to see the file in Windows Explorer, the SYSTEM account, which DNA uses, does not have adequate permissions to access the network file.	You must have administrator rights to access the file so that the Distributed Network Attack (DNA) Server, which runs as a System service, can also access the file. Copy the network file to the local machine. Add the file to DNA.
Why is a DNA Worker not responding?	The DNA Worker lost its connection to the network or is turned off.	Try to ping the DNA Worker machine from the DNA Supervisor machine. If you can ping the Worker machine, but the DNA Worker is still not responding, first, try restarting the DNA worker from the machine it is running on. If that does not work, reboot the computer that is running the DNA Worker. If you cannot ping the Worker machine, verify that the worker machine is turned on, and try to access network services on it, such as the Internet or printing. If the DNA Worker is still not responding, see the system administrator or call AccessData.

TABLE 11-3 DNA Troubleshooting FAQs

Problem	Possible Cause	Solution
	The **Stop Worker on User Input** option has been selected.	Uncheck the option.
After I added a job and DNA worked on it, the Password/ User Password column read "Empty Password." Why?	The file is encrypted, but the password is empty or contains no characters.	To unlock the file, press **Enter** when you are prompted for a password.
I added a job, and DNA has still not located the password. Why?	Finding passwords can take a long time, depending on the attack type. Keyspace attacks can take a very long time, depending on the size of the keyspace. A password may not be recovered if it is not contained within the selected dictionaries, or covered by Rules you have selected for the job.	Install more DNA Workers with at least the recommended processor requirements. The more machines that DNA can use, the faster it can run its tests. Gather as much information as you can find and add it to a biographical dictionary. This helps to ensure the password or pass-phrase will be found.
What is the difference between the owner keys and passwords and the user keys and passwords?	PDF documents have both owner and user passwords. The owner password is used to open and edit the file. The user password is used to open and read the file.	Use either the owner or user password to unlock the PDF document. Generally, you use the user password to unlock the document. However, in some instances you might use the owner password to modify the file. For example, if the file creator has forgotten the password, you might create a new password for the file.

ADD JOB PROCESSING RESULTS

After processing jobs to be added, PRTK displays results in the Processing results dialog. The following are possible results:

TABLE 11-4 Available Add Job Processing Results

Result	Description
Cancelled	You canceled the processing of the job.
Corrupted	The file is corrupted.
Failed to Process	The file cannot be added to the system. This result is a general tag used for any file that cannot be classified as any other result.
File in Use	The file is locked by another program.
Successfully Added	The file is added to the job queue.
Timed Out	The file cannot be identified by PRTK in five minutes. This result usually appears when PRTK is busy processing other jobs.
Unencrypted	The file doesn't need to be added because the file isn't encrypted.
Unidentifiable	PRTK cannot recognize the file and its source application.
Unsupported Version	The file was created in an unsupported version of a supported application.

For additional troubleshooting information, contact AccessData Customer Support by emailing your questions to support@accessdata.com, or use the Forensic Forum on the AccessData Web site.

Appendix A Recognized Applications and File Formats

This appendix lists the applications and file formats that Password Recovery Toolkit® (PRTK®) 6.5 and Distributed Network Attack® (DNA®) 3.5 recognizes, and their corresponding modules.

The appendix is divided into sections based on the attack type that PRTK uses to decrypt the file. The last section lists applications that use multiple attack types.

DECRYPTION ATTACK

The decryption attack decrypts the password that locks the file. PRTK uses the decryption attack on the applications listed in the following table.

TABLE A-1 PRTK and DNA Decryption Attack Modules

Supported Application	Module
7-Zip - Support for 4.65, 9.4 -9.10, PS3 Support	7-Zip Decryption Module
ACT! 1–4, 2000, 5–6	ACT! Decryption Module
Adobe Acrobat 3.0–6.0 and Adobe PDF 1.2–1.6	PDF Decryption Module
AOL Desktop Client 8.0–9.0 Security Edition	AOL Password Module
AOL Instant Messanger through 5.9, 6.9, 7.1, AIM Triton through 1.0.4	AIM Password Module
Ascend	Ascend Password Module
BulletProof FTP 1.03–2.45	BPFTP Password Module

TABLE A-1 PRTK and DNA Decryption Attack Modules

Supported Application	Module
Chrome (Google)	Google Chrome Decryption Module
CuteFTP 2–5, 7*x*	CuteFTP Password Module
DataPerfect	DataPerfect Password Module
dBASE 2.*x*–3.*x*	dBASE Password Module
EasyCrypto 5.5 -- File decryption upon completion	EasyCrypto Password Module
FileMaker 3.*x*, 5.*x*	FileMaker Password Module
Hello 1.0	Hello Password Module
ICQ 2003b–5.04	ICQ Password Module
Internet Explorer 5.0–6.0 AutoComplete database	Protected Registry Module This module is also used for Outlook Express.
Kaikei through 05	Kaikei Password Module
Lotus 1-2-3 of the following versions: 1A–4 9 97 FRM Japanese	Lotus 123 Password Module This module is also used for Lotus Symphony 1–2 and Lotus 1-2-3 seal passwords.
Lotus 1-2-3 seal passwords	Lotus 123 Password Module This module is also used for Lotus Symphony and Lotus 1-2-3.
Lotus Approach thorugh 97	Lotus Approach Password Module
Lotus Notes, version 8.5	
Lotus Organizer 1–4	Lotus Organizer Password Module
Lotus Symphony 1–2	Lotus 123 Password Module This module is also used for Lotus 1-2-3 and Lotus 1-2-3 seal passwords.
Lotus WordPro 96, 97, or Millenium	WordPro Password Module
Messenger Plus! 3.50–3.61, 4.82 & 4.83	MessengerPlus Password Module
Microsoft Access	MS Access Encryption Module
Microsoft Money 2002–2006	MS Money Password Module
Microsoft Office Data (PST) files 2007 or earlier	MS Outlook PST Password Module

TABLE A-1 PRTK and DNA Decryption Attack Modules

Supported Application	Module
Microsoft Office Excel 2–7, 97 through 2007 Word 2–6, 97 through 2007 PowerPoint XP through 2007	Microsoft Office Encryption Module
Microsoft Project 98–2003	MS Project Password Module
Microsoft Schedule+ 7.*x*	Scheduler Password Module
Microsoft SourceSafe 6*x*	SourceSafe Password Module
Microsoft Visual SourceSafe 6.*x*	SourceSafe Password Module
MozillaProtectedData Mozilla 1.7x AOL Communicator through 20030919.3 Mozilla Firefox through 1.5 Netscape 7.*x*–8.0	Mozilla Protected Data Module
MS Backup	MS Backup Password Module
MS Mail	MS Mail Password Module
MSN Messenger through 7.0	MSN Messenger Password Module
MYOB Plus 3.*x* Premier Accounting 2005–2006 Business Basics 2	MYOB Password Module
Netscape Mail through 6.*x*	Netscape Mail Password Module
Outlook Express 5.0–6.0, SMTP password	Protected Registry Module This module is also used for Internet Explorer.
Palm Pilot User File	Palm Password Module
Paradox 4.*x*, 5.*x*, or 7.*x*	Paradox Password Module
PasswordPal through 2.0	PasswordPal Password Module
Protected Registery, now supports: Windows 7, TACC, and PS3 Microsoft Internet Explorer 5.0–6.0 Microsoft Outlook Express 5.0–6.0	Protected Registry Module
ProWrite	ProWrite Password Module
PCEncrypt through 9.11	PCEncryption Encryption Module
PST through 2007	MS Outlook PST Password Module
PWL	PWL Password Module
Quattro Pro 1–12, X3	Quattro Pro Password Module

TABLE A-1 PRTK and DNA Decryption Attack Modules

Supported Application	Module
Quickbooks through 2010	Quickbooks Password Module
Quicken through 2001	Quicken Password Module
SAMFile - 10.6 SAM Files LAN Hash, NT Hash (MD4) Active Directory	SAM File Module
Steganos Security Suite LockNote	Steganos Password Module
Symantec QA 4.*x*–5.*x*	SymantecQA Password Module
VBA	VBA Password Module
VersaCheck VersaCheck 2001 Home and Pro VersaCheck Platinum 2004–2007 VersaCheck Enterprise 2004–2007 2010	VersaCheck Password Module
Whisper 32 1.16 or earlier	Whisper Password Module
Windows 95 Screen Saver	Screen Saver Password Module
Windows XP Credential Files in Windows XP through Service Pack 2	XP Credentials Module
WordPerfect 5.0–12, X3	WordPerfect Password Module
WS_FTP 5.0*x*, 2006	WS_FTP Encryption Module
Yahoo! Messenger 3.0–7.0	Yahoo! Messenger Password Module
Yayoi Kaikei 05 or earlier	Kaikei Password Module

DICTIONARY ATTACK

The dictionary attack uses the words in a dictionary, applies Rules to the words, and applies the password to the files. PRTK uses the dictionary attack on the applications listed in the following table.

TABLE A-2 PRTK and DNA Dictionary Attack Modules

Supported Application	Module
7-Zip 4.65, 9.4-9.10, PS3	7-Zip Password Module
ABI Coder 3.5.7.4–3.6.1.4	ABI Coder Password Module
Advanced File Lock 7.1	AdvancedFileLock Password Module

TABLE A-2 PRTK and DNA Dictionary Attack Modules

Supported Application	Module
Adobe Acrobat 3.0–6.0 and Adobe PDF 1.2–1.6	PDF Encryption Module
AOL Instant Messenger through 5.9, AIM Triton through 1.0.4	AIM Password Module
Ami Pro	AmiPro Password Module
ARJ 2.82	ARJ Password Module
Ashampoo Security Manager 99 Power Encrypt Privacy Protector through 2005 Magic Security	Ashampoo Password Module
BestCrypt 4.*x*–8.20, BCArchive 1.06	BestCrypt Password Module
CD-Lock Support through 9.50, first 32k needed for unlock.exe	CDLock Password Module
CheckWriter 5.*x*	CheckWriter Password Module
CodedDrag 2.4	CodedDrag Password Module
crypt htpasswd passwd MD5-based, SHA-based, fcrypt	*nix crypt Password Module
fcrypt; MD5, SHA-1, Blowfish, SHA-256, and SHA-512 based crypt	
PS3 for SHA-256 and SHA-512 based crypt	
Cryptainer LE 5–6	Cryptainer Password Module
CryptaXix CryptaPix 2.00–3.05 CryptaFlix 1.00–3.05	CryptaXix Password Module
CrypText 2.30–3.40	CrypText Password Module
CuteFTP 2–5, 7*x*	CuteFTP Password Module
DriveCrypt 4.2	DriveCrypt Password Module
DriveCrypt Plus Pack 3.0	DriveCrypt Plus Pack Password Module
Encrypted Magic Folders 3.x, 7.x -- 9.06	EMF Password Module
Geli	Geli Password Module
New module, 1 through 3. Geli first appeared in Free BSD 6.0. Support has been tested in the latest version, 8.0.	

TABLE A-2 PRTK and DNA Dictionary Attack Modules

Supported Application	Module
GnuPG 1.4.0 or earlier	PGP Password Module This module is also used for PGP.
HandyBits EasyCrypto Delux 5.5 -- File decryption upon completion.	EasyCrypto Password Module
htpasswd	*nix crypt Password Module This module is also used for passwd.
Icon Lock-IT XP	Lockit Password Module
Internet Explorer Content Advisor, version 8	IEContent Password Module
Justsystem Ichitaro 5–2004 Hanako 3.1–2004	Justsystem Password Module
KeyChain	KeyChain Password Module
KeePass Password Safe 8–1.04, 2.08, 2.09, 3.20	KeePass Password Module
Kremlin Encrypt 3.0, Text 3.0 File decryption upon completion	Kremlin Password Module
MaxCrypt 1.0–1.10	MaxCrypt Password Module
Messenger Plus! 3.50–3.61, 4.82 & 4.83	MessengerPlus Password Module
Microsoft Encrypted File System (EFS), Windows 2000 through Windows 7	EFS Module
Microsoft Office Excel 2–7, 97 through 2007 Word 2–6, 97 through 2007 PowerPoint XP through 2007	Microsoft Office Encryption Module
Microsoft Money 2002–2006	MS Money Password Module
Mozilla Mozilla 1.7*x* AOL Communicator 20030919.3 FireFox through 1.5 Netscape 7.*x*–8.0	Mozilla Master Password Module
MYOB Plus 3.*x* Premier Accounting 2005–2006 Business Basics 2	MYOB Password Module
Norton Secret Stuff 1.0	SecretStuff Encryption Module
Omziff 1.0–3.0.4	Omziff Password Module

TABLE A-2 PRTK and DNA Dictionary Attack Modules

Supported Application	Module
OpenOffice.org Office 1.0–3.1 StarOffice	OpenOffice Password Module
passwd, MD5- and SHA-based encryption and fcrypt	*nix crypt Password Module This module is also used for htpasswd.
PasswordPal through 2.0	PasswordPal Password Module
PasswordSafe 1–3	PasswordSafe Password Module
PC-Encrypt through 9.11	PCEncrypt Encryption Module
PDF Acrobat 3.0–9.0, all file types PDF 1.2–1.6	PDF Encryption Module
PFX Microsoft PFX P12 Private Key Format	PFX Password Module
PGP PGP 9.0.2 gnupg 1.4.0	PGP Password Module
PGP Disk PGP 8.1or earlier PGP Disk 4.0–6.0 PGP SDA Whole Disk Encryption 9.0	PGP Disk Password Module
PKZIP	ZIP Password Module This module is also used for WinZip 8 or earlier.
PWL	PWL Password Module
Quickbooks 2003–2010	Quickbooks Password Module
Quicken 2003–2006	Quicken Password Module
RAR 1.*x*–3.*x*	RAR Password Module
SafeHouse Personal Privacy 2, versions 3.04 & 3.06	SafeHouse Password Module
SAM files - 10.6 SAM files NT (MD4) hash, LAN hash Active Directory	SAM File Module
SecureIT 3.1 -- 4.0	SecureIT Password Module
SecretStuff 1.0	SecretStuff Encryption Module
SiFEU File Encryptor 0.9	SiFEU Password Module

TABLE A-2 PRTK and DNA Dictionary Attack Modules

Supported Application	Module
Steganos 2009 Security Suite LockNote	Steganos Password Module
S-Tools - Removed	Functionality is now found in Steganography module
VBA	VBA Password Module
WinZip 9.0–14	WinZip9 Password Module
ZIP WinZip PKZIP 8 - 12.4	ZIP Password Module

KEYSPACE ATTACKS

The keyspace attack is used on applications that use 40-bit encryption or less. Because of the relatively small number of possible keys, DNA tries every possible key until it finds the one that decrypts the file.

Some applications use the keyspace attack in conjunction with another attack. For more information, see "Multiple Attacks."

TABLE A-3 PRTK and DNA Keyspace Attack Modules

Supported Application	Module
AOL Instant Messanger through 5.9, AIM Triton through 1.0.4	AIM Password Module
ARJ 2.82	ARJ Password Module
CryptaXix CryptaPix 2.00–2.24 CryptaFlix 1.00–1.10	CryptaXix Password Module
ICQ 2003b–5.04	ICQ Password Module
Microsoft Office Excell 2–7, 97,2000, XP, 2003 Word 2–6, 97,2000, XP, 2003 PowerPoint XP, 2003	Microsoft Office Encryption Module
PDF Acrobat 3.0–6.0 PDF 1.2–1.6	PDF Encryption Module
PWL	PWL Password Module

TABLE A-3 PRTK and DNA Keyspace Attack Modules

Supported Application	Module
SAM files, 10.6 SAM files NT (MD4) hash, LAN hash Active Directory	SAM File Module
SecretStuff 1.0	SecretStuff Encryption Module
ZIP WinZip 9 - 14 PKZIP 8	ZIP Password Module

RESET ATTACKS

Reset attack is the least common attack type used by PRTK because few applications are susceptible to it.

TABLE A-4 Reset Attack Modules

Supported Application	PRTK Module
Ashampoo Security Manager 99 Power Encrypt Privacy Protector through 2005 Magic Security	Ashampoo Password Module
DriveCrypt 4.2	DriveCrypt Password Module
MSN Messenger through 7.0	MSN Messenger Password Module
MYOB Plus 3.*x* Premier Accounting 2005–2006 Business Basics 2	MYOB Password Module
Quickbooks 2003–2010	Quickbooks Password Module
Quicken 2003–2006	Quicken Password Module
VBA	VBA Password Module

MULTIPLE ATTACKS

Some applications are susceptible to more than one attack type. Multiple attacks can be used to decrease the time necessary to decrypt a file. For applications where multiple attack types can be used, PRTK starts with the least time-consuming attack type.

For example, PRTK might use a dictionary attack first on a PowerPoint spreadsheet and then use the key space attack if the file isn't decrypted during the dictionary attack.

PRTK uses multiple attack types on the applications listed in the following table. The order in which the attack types are listed in the table is the order that PRTK uses.

TABLE A-5 PRTK and DNA Multiple Attack-Type Modules

Supported Application	Attack Types	PRTK Module
AOL 8.0–9.0 Security Edition	Decryption Keyspace	AOL Password Module
AOL Communicator 20030919.3 or earlier	Dictionary Decryption	The dictionary attack uses the Mozilla Master Password Module. This module is also used for Mozilla, Mozilla Firefox, and Netscape. The decryption attack uses the Mozilla Protected Data Module. This module is also used for Mozilla, Mozilla Firefox, and Netscape.
ARJ 2.82 or earlier	Keyspace Dictionary	ARJ Password Module
DriveCrypt 4.2 through 5.4	Dictionary Reset	DriveCrypt Password Module
HandyBits EasyCrypto Deluxe 5.5 -- File decryption upon completion	Dictionary Decryption	EasyCrypto Password Module
Microsoft Excel 2–7, 97, 2000, XP, 2003	Dictionary Decryption	Microsoft Office Encryption Module This module is also used for Microsoft Word and Microsoft PowerPoint.

TABLE A-5 PRTK and DNA Multiple Attack-Type Modules

Supported Application	Attack Types	PRTK Module
Microsoft Money 97–2004, backup files	Dictionary Decryption Versions of Microsoft Money before 2002 use the decryption attack. Microsoft Money 2002–04 uses the dictionary attack.	MS Money Password Module
Microsoft PowerPoint XP and 2003	Dictionary Decryption	Microsoft Office Encryption Module This module is also used for Microsoft Excel and Microsoft PowerPoint.
Microsoft Word 2–6, 97, 2000, XP, and 2003	Dictionary Decryption	Microsoft Office Encryption Module This module is also used for Microsoft Excel and Microsoft PowerPoint.
Mozilla 1.7.*x* Also between 7.0 & 9.0	Dictionary Decryption	The dictionary attack uses the Mozilla Master Password Module. This module is also used for AOL Communicator, Mozilla Firefox, and Netscape. The decryption attack uses the Mozilla Protected Data Module. This module is also used for AOL Communicator, Mozilla Firefox, and Netscape.

TABLE A-5 PRTK and DNA Multiple Attack-Type Modules

Supported Application	Attack Types	PRTK Module
Mozilla Firefox 1.0.4 or earlier	Dictionary Decryption	The dictionary attack uses the Mozilla Master Password Module. This module is also used for AOL Communicator, Mozilla, and Netscape. The decryption attack uses the Mozilla Protected Data Module. This module is also used for AOL Communicator, Mozilla, and Netscape.
Netscape 7.*x*–8.0	Dictionary Decryption	The dictionary attack uses the Mozilla Master Password Module. This module is also used for AOL Communicator, Mozilla, and Mozilla Firefox. The decryption attack uses the Mozilla Protected Data Module. This module is also used for AOL Communicator, Mozilla, and Mozilla Firefox.
Password Pal 2.0 or earlier	Dictionary Decryption	PasswordPal Password Module
QuickBooks 2001 or earlier	PRTK uses a decryption attack to recover the file passwords for QuickBooks 2001 or earlier. To open a recovered file, open it in QuickBooks and enter the recovered password when prompted.	QuickBooks Password Module

TABLE A-5 PRTK and DNA Multiple Attack-Type Modules

Supported Application	Attack Types	PRTK Module
QuickBooks 2003–2004	PRTK resets the file passwords for QuickBooks 2003–2004. To open a recovered file, open it in QuickBooks and enter a blank password when prompted.	QuickBooks Password Module
Quicken 2004 or earlier	Dictionary Decryption Reset PRTK uses a dictionary attack to recover the file passwords for Quicken 2003–2004. A decryption attack is used for Quicken 2001 or earlier. PRTK resets the password to a blank password for Quicken 2002.	Quicken Password Module
Visual Basic for Applications (VBA)	Dictionary Decryption Reset	VBA Password Module
Windows PWL files	Decryption Dictionary	PWL Password Module
WinZip 8 or earlier	Keyspace Dictionary	ZIP Password Module This module is also used for PKZIP.

Appendix B
Password Recovery Attacks

A profile is the combination of four individual components: Languages, Character Groups, Dictionaries, and Rules, each described below.

LANGUAGES

Language selection affects two aspects of password recovery: the dictionaries selected for dictionary attacks (which can also be independently selected and deselected), and the character sets that will be used in Rules that use computer generated characters as opposed to reading words from a dictionary. PRTK 6.5 and DNA 3.5 currently support the following character sets: Arabic, English, French, German, Italian, Russian and Spanish.

CHARACTER GROUPS

Character groups allow a profile to refine and expand the set of characters that will be used in Rules that generate characters. The following character groups can be selected or deselected for the given profile:

TABLE B-1 Available Character Groups

Character Group	Description
All 7-bit Characters (ASCII)	Character represented by a value from 0 to 127 encoded as a byte.
All 8-bit Characters	Character represented by a value from 0 to 255 encoded as a byte.

TABLE B-1 Available Character Groups

Character Group	Description
Uppercase Letters	Characters represented as uppercase for the selected languages in the profile (for languages that support uppercase and lowercase characters).
Lowercase Letters	Characters represented as lowercase for the selected languages in the profile (for languages that support uppercase and lowercase characters).
Diacritics	The combination of a character and an additional mark sometimes referred to as an accent.
Digits	Characters represented as numbers for the selected languages in the profile (for languages that support digit characters).
Symbols (Standard)	Non-Alphanumeric characters that can be found on a keyboard.
Symbols (Extended)	Non-Alphanumeric characters that cannot be found on a keyboard. Characters selected from the character map utility provided in Microsoft Windows, for example.

DEFAULT DICTIONARIES

Dictionaries are word list groupings that have been complied in several different languages in both a codepage and Unicode format. PRTK6.5 and DNA 3.5 will select the correct format depending on whether a module uses codepage or Unicode. Once a dictionary has reached 500,000 entries, a new codepage and Unicode dictionary is created.

PRTK 6.5 and DNA 3.5 ship with the following dictionaries:

TABLE B-2 Default Dictionaries Listed by Default Language Profile

Language	Format
Arabic	[AR-1] Names-ar-c.adf: Arabic Names (codepage)
	[AR-1] Names-ar-u.adf: Arabic Names (Unicode)
	[AR-2] Quran-ar-c.adf: Arabic words from the Quran (codepage)
	[AR-2] Quran-ar-u.adf: Arabic words from the Quran (Unicode)
	[AR-3] General-ar-c.adf: General Arabic words (codepage)
	[AR-3] General-ar-u.adf: General Arabic words (Unicode)

TABLE B-2 Default Dictionaries Listed by Default Language Profile

Language	Format
German	[DE-1] General-1-de-c.adf: General German words – List 1 (codepage)
	[DE-1] General-1-de-u.adf: General German words – List 1 (Unicode)
	[DE-1] General-2-de-c.adf: General German words – List 2 (codepage)
	[DE-1] General-2-de-u.adf: General German words – List 2 (Unicode)
	[DE-1] General-3-de-c.adf: General German words – List 3 (codepage)
	[DE-1] General-3-de-u.adf: General German words – List 3 (Unicode)
	[DE-1] General-4-de-c.adf: General German words – List 4 (codepage)
	[DE-1] General-4-de-u.adf: General German words – List 4 (Unicode)
English	[EN-1] Common-en-c.adf: Common English words and passwords (codepage)
	[EN-1] Common-en-u.adf: Common English words and passwords (Unicode)
	[EN-2] Miscellaneous-en-c.adf: Crime related, keyboard sequences and words that may not be found in normal dictionaries (codepage)
	[EN-2] Miscellaneous-en-u.adf: Crime related, keyboard sequences and words that may not be found in normal dictionaries (Unicode)
	[EN-3] Names-en-c.adf: Common English first names, last names and business names (Codepage)
	[EN-3] Names-en-u.adf: Common English first names, last names and business names (Unicode)
	[EN-4] General-1-en-c.adf: General English words, not found in the other English dictionaries – List 1 (codepage)
	[EN-4] General-1-en-u.adf: General English words, not found in the other English dictionaries – List 1 (Unicode)
	[EN-4] General-2-en-c.adf: General English words, not found in the other English dictionaries – List 2 (codepage)
	[EN-4] General-2-en-u.adf: General English words, not found in the other English dictionaries – List 2 (Unicode)
Spanish	[ES-1] General-es-c.adf: General Spanish words (codepage)
	[ES-1] General-es-u.adf: General Spanish words (Unicode)
French	[FR-1] General-fr-c.adf: General French words (codepage)
	[FR-1] General-fr-u.adf: General French words (Unicode)
Italian	[IT-1] General-it-c.adf: General Italian words (codepage)
	[IT-1] General-it-u.adf: General Italian words (Unicode)

TABLE B-2 Default Dictionaries Listed by Default Language Profile

Language	Format
Japanese	[JA-1] Hiragana-ja-c.adf: Japanese words from the Hiragana dialect (codepage)
	[JA-1] Hiragana-ja-u.adf: Japanese words from the Hiragana dialect (Unicode)
	[JA-2] Kanji-ja-c.adf: Japanese words from the Kanji dialect (codepage)
	[JA-2] Kanji-ja-u.adf: Japanese words from the Kanji dialect (Unicode)
	[JA-3] Katakana-ja-c.adf: Japanese words from the Katakana dialect (codepage)
	[JA-3] Katakana-ja-u.adf: Japanese words from the Katakana dialect (Unicode)
Russian	[RU-1] General-1-ru-c.adf: General Russian words – list 1 (codepage)
	[RU-1] General-1-ru-u.adf: General Russian words – list 1 (Unicode)
	[RU-1] General-2-ru-c.adf: General Russian words – list 2 (codepage)
	[RU-1] General-2-ru-u.adf: General Russian words – list 2 (Unicode)
Slovak	[SK-1] General-sk-c.adf: General Slovak words (codepage)
	[SK-1] General-sk-u.adf: General Slovak words (Unicode)

RULES

Rules create password tests that are:

- Words that are read from dictionaries
- Characters that are computer generated
- A combination of both

This table lists the intensity of each Rule:

TABLE B-3 Basic, Advanced, and Pass Phrase Rules Differences

Attempt Category	Attempt Intensity
Basic (BAS)	1—Less than one-million tests
	2—One-million to one-billion tests
	3—One-billion to ten-billion tests
Advanced (ADV)	1—Ten-billion to 25-billion tests
	2—25-billion to 50-billion tests
	3—50-billion to 100-billion tests
	4—More than 100-billion tests

TABLE B-3 Basic, Advanced, and Pass Phrase Rules Differences

Attempt Category	Attempt Intensity
Pass Phrase (PP)	1—Less that 100-billion tests
	2—100-billion to one-trillion tests
	3—More than one-trillion tests

DEFAULT RULE ORDER

Rule order can be changed, rearranged to meet your specific needs. This table shows the default Rule order for new profiles:

TABLE B-4 PRTK 6.5 & DNA 3.5 Default Rule Order

Rule	Description	Example
(BAS-1-01)	One digit search	9
(BAS-1-02)	One letter, language specific search	b
(BAS-1-03)	Two digit search	33
(BAS-1-04)	Two letter, language specific search	XP
(BAS-1-05)	Three digit search	456
(BAS-1-06)	Three letter, language specific search	aBc
(BAS-1-07)	Four digit search	9876
(BAS-1-08)	Five digit search	15935
(BAS-1-09)	Five Markov characters within a threshold of one hundred with two characters upper cased search	
(BAS-1-10)	Six digit search	123456
(BAS-1-11)	Four Markov characters with a threshold of one primary search	
(BAS-2-01)	Four letter, language specific search	ZXcv
(BAS-2-02)	Five letter, language specific search	LKJhg
(BAS-2-03)	Five Markov characters with a threshold of one primary search	revid
(BAS-2-04)	Five Markov characters with a threshold of one primary reverse search	elpa
(BAS-2-05)	Six Markov characters with a threshold of one primary search	clorne
(BAS-2-06)	Six Markov characters with a threshold of one hundred with two characters upper cased search	

TABLE B-4 PRTK 6.5 & DNA 3.5 Default Rule Order

Rule	Description	Example
(BAS-2-07)	Six Markov characters with a threshold of one primary reverse search	enrolc
(BAS-2-08)	Seven digit search	7777777
(BAS-2-09)	Seven Markov characters with a threshold of fifty primary search	drotune
(BAS-2-10)	Seven Markov characters with a threshold of fifty primary reverse search	enutord
(BAS-2-11)	Seven Markov characters with a threshold of one hundred with two characters upper cased search	
(BAS-2-12)	Seven digit telephone number search	555-1234
(BAS-2-13)	Eight digit search	98765432
(BAS-2-14)	Eight Markov characters with a threshold of fifty primary search	schroten
(BAS-2-15)	Eight Markov characters with a threshold of fifty primary reverse search	netorhcs
(BAS-2-16)	Eight Markov characters with a threshold of one hundred with two characters upper cased search	
(BAS-2-17)	Dictionary primary search	Apple
(BAS-2-18)	Dictionary primary reverse search	llabesab
(BAS-2-19)	Dictionary with two characters upper cased search	peACh
(BAS-2-20)	Dictionary primary character replacements search	b@n@n@
(BAS-2-21)	Dictionary primary followed by common postfixes search	jazz#1
(BAS-2-22)	Dictionary primary preceded by common prefixes search	drBob
(BAS-2-23)	Dictionary primary followed by a one digit search	orange2
(BAS-2-24)	Dictionary primary preceded by a one digit search	1pear
(BAS-2-25)	Dictionary primary followed by a one letter, language specific search	strawberryQ
(BAS-2-26)	Dictionary primary preceded by a one letter, language specific search	xCherry
(BAS-2-27)	Dictionary primary followed by a non-alphanumeric symbol search	plum$
(BAS-2-28)	Dictionary primary preceded by a language-specific non-alphanumeric symbol search	^raspberry
(BAS-2-29)	Dictionary primary character replacement, followed by a one digit search	@pple5

TABLE B-4 PRTK 6.5 & DNA 3.5 Default Rule Order

Rule	Description	Example
(BAS-2-30)	Dictionary primary character replacement, preceded by a one digit search	3Pea[h
(BAS-2-31)	Dictionary primary preceded and followed by a one digit search	4orange4
(BAS-2-32)	Dictionary primary followed by a two digits search	bANANA55
(BAS-2-33)	Dictionary primary preceded by a two digits search	12CHERRY
(BAS-2-34)	Dictionary primary preceded by common prefixes and followed by a one digit search	mrAnderson1
(BAS-2-35)	Dictionary primary preceded by one digit followed by common postfixes	3cat's
(BAS-2-36)	Date Search (Two digit year)	12-17-83
(BAS-2-37)	Three letter, language specific characters followed by common postfixes	trw123
(BAS-2-38)	Three letter, language specific characters preceded by common prefixes	abcmgh
(BAS-2-39)	Five Markov Characters with a threshold of one followed by common postfixes	revid123
(BAS-2-40)	Five Markov Characters with a threshold of one preceded by common prefixes	abcrevid
(BAS-2-41)	Six Markov Characters with a threshold of fifty followed by common postfixes	
(BAS-2-42)	Six Markov Characters with a threshold of fifty preceded by common prefixes	
(BAS-2-43)	Nine Markov characters with a threshold of one hundred search	
(BAS-3-01)	Dictionary primary with a non-alphanumeric symbol inserted search	app&le
(BAS-3-02)	Dictionary primary character replacement, followed by a two digit search	@apple23
(BAS-3-03)	Dictionary primary character replacement, preceded by a two digit search	76app|e
(BAS-3-04)	Dictionary primary followed by a three digit search	apple258
(BAS-3-05)	Dictionary primary preceded by a three digit search	987apple
(BAS-3-06)	Social Security Number Search	123-45-6789
(BAS-3-07)	Four letter, language specific characters preceded by common prefixes	abcPoUy

TABLE B-4 PRTK 6.5 & DNA 3.5 Default Rule Order

Rule	Description	Example
(BAS-3-08)	Four letter, language specific characters followed by common postfixes	Asdf123
(ADV-1-01)	All one-character, language-specific search	a
(ADV-1-02)	All two character, language-specific search	1a
(ADV-1-03)	All three-character, language-specific search	!1a
(ADV-1-04)	All four-character, language-specific search	1a%
(ADV-1-05)	One digit followed by three language-specific characters search	7!qy
(ADV-1-06)	Three language-specific characters followed by one digit search	tuh5
(ADV-1-07)	One language-specific character followed by a four digit search	*1234
(ADV-1-08)	One digit followed by four language-specific characters search	5wert
(ADV-1-09)	Two language-specific characters followed by a three digit search	xx333
(ADV-1-10)	Two digits followed by three language-specific characters search	93!Q2
(ADV-1-11)	Three language-specific characters followed by a two digit search	!@d56
(ADV-1-12)	Four language-specific characters followed by a one digit search	A$Df6
(ADV-1-13)	Four language-specific characters followed by a non-alphanumeric symbol search	P0&6@
(ADV-1-14)	Four language-specific characters preceded by a non-alphanumeric symbol search	$t7^3
(ADV-1-15)	Six letter, language specific search	QwErTy
(ADV-1-16)	Two digits followed by four language-specific characters search	22asD%
(ADV-1-17)	Two language-specific characters followed by four digits search	$%1234
(ADV-1-18)	Three language-specific characters followed by a three digit search	4%$123
(ADV-1-19)	Four language-specific characters followed by a two digit search	Aa4$77

TABLE B-4 PRTK 6.5 & DNA 3.5 Default Rule Order

Rule	Description	Example
(ADV-1-20)	Dictionary primary followed by a two letter, language specific search	Appleff
(ADV-1-21)	Dictionary primary preceded by a two letter, language specific search	quapple
(ADV-1-22)	Dictionary primary preceded by a two digit followed by common postfixes	12appleabc
(ADV-1-23)	Dictionary primary preceded by common prefixes and followed by a two digit search	abcapple12
(ADV-1-24)	Dictionary primary preceded and followed by a two digit search	12apple34
(ADV-1-25)	Dictionary primary followed by a four digit search	apple4567
(ADV-1-26)	Dictionary primary preceded by a four digit search	2468apple
(ADV-1-27)	Ten digit telephone number search	800-555-8888
(ADV-2-01)	All five-character, language-specific search	Hg^(s
(ADV-3-01)	Four language-specific characters with a non-alphanumeric symbol inserted search	a3&c8
(ADV-3-02)	Four language-specific characters followed by a three digit search	r6zg555
(ADV-4-01)	All six-character, language-specific search	Dg*4g&
(ADV-4-02)	Seven letter search	aAbBcCd
(ADV-4-03)	All seven-character, language-specific search	a1!c$t7
(ADV-4-04)	Eight letter search	sLdKIenD
(ADV-4-05)	All eight-character, language-specific search	!@#$12we
(ADV-4-06)	Nine letter, language specific search	aISODheKg
(ADV-4-07)	All nine-character, language-specific search	*&g1234
(ADV-4-08)	Ten letter, language specific search	SOdkghdlSJ
(ADV-4-09)	All ten-character, language-specific search	1a!2b@3c#4
(ADV-4-10)	All eleven-character, language-specific search	1a!2b@3c#4D
(ADV-4-11)	All twelve-character, language-specific search	1a!2b@3c#4D $
(PP-1-01)	Two word concatenation without spaces search	dogcat
(PP-1-02)	Two word concatenation with spaces search	cat dog

If you create additional Rules, more Rules are added to the password attacks. If you select Customized Dictionaries, more Rules will be added to the attack.

PROFILES

DNA and PRTK share the same profile names, though the DNA Profiles use additional Rules (suggested for distributed processing only). These Profiles are discussed in detail later in this chapter.

TABLE B-5 PRTK & DNA Default Profiles

Profile Name	Profile Name
• English (default)	• Pass-phrase
• English Transitional	• FTK Import
• Arabic	• PRTK
• European	• DNA
• Russian	

ENGLISH

The English profile begins by searching for simple passwords, followed by, dictionary and permutated dictionary searches, and ends with complex searches for dictionary and computed password. The program uses all default English dictionaries and character sets.

DICTIONARIES:

TABLE B-6 Default Dictionaries for the English Profile

Dictionary Name	Dictionary Name
[EN-1] Common-en-c.adf	[EN-3] Names-en-u.adf
[EN-1] Common-en-u.adf	[EN-4] General-1-en-c.adf
[EN-2] Miscellaneous-en-c.adf	[EN-4] General-1-en-u.adf
[EN-2] Miscellaneous-en-u.adf	[EN-4] General-2-en-c.adf
[EN-3] Names-en-c.adf	[EN-4] General-2-en-u.adf

RULES (IN DEFAULT ORDER)

1. (BAS-1-01) One digit search
2. (BAS-1-03) Two digit search
3. (BAS-1-05) Three digit search

4. (BAS-1-07) Four digit search
5. (BAS-1-08) Five digit search
6. (BAS-1-02) One letter, language specific search
7. (BAS-1-04) Two letter, language specific search
8. (BAS-1-06) Three letter, language specific search
9. (ADV-1-01) All one-character, language-specific search
10. (BAS-1-11) Four Markov characters with a threshold of one primary search
11. (BAS-2-03) Five Markov characters with a threshold of one primary search
12. (BAS-2-17) Dictionary primary search
13. (BAS-2-01) Four letter, language specific search
14. (BAS-2-04) Five Markov characters with a threshold of one primary reverse search
15. (ADV-1-07) One language-specific character followed by a four digit search
16. (BAS-1-10) Six digit search
17. (BAS-2-36) Date Search (two digit year)
18. (ADV-1-03) All three-character, language-specific search
19. (BAS-2-05) Six Markov characters with a threshold of one primary search
20. (BAS-2-09) Seven Markov characters with a threshold of fifty primary search
21. (BAS-2-21) Dictionary primary followed by common postfixes search
22. (BAS-2-22) Dictionary primary preceded by common prefixes search
23. (BAS-2-23) Dictionary primary followed by a one digit search
24. (BAS-2-24) Dictionary primary preceded by a one digit search
25. (BAS-2-25) Dictionary primary followed by a one letter, language specific search
26. (BAS-2-26) Dictionary primary preceded by a one letter, language specific search
27. (BAS-2-20) Dictionary primary character replacements search
28. (BAS-2-13) Eight digit search
29. (BAS-2-12) Seven digit telephone number search
30. (ADV-1-05) One digit followed by three language-specific characters search
31. (ADV-1-06) Three language-specific characters followed by one digit search
32. (BAS-2-10) Seven Markov characters with a threshold of fifty primary reverse search
33. (BAS-2-02) Five letter, language specific search
34. (ADV-1-17) Two language-specific characters followed by four digits search
35. (BAS-2-14) Eight Markov characters with a threshold of fifty primary search

36. (BAS-2-15) Eight Markov characters with a threshold of fifty primary reverse search
37. (BAS-2-27) Dictionary primary followed by a non-alphanumeric symbol search
38. (BAS-2-28) Dictionary primary preceded by a language-specific non-alphanumeric symbol search
39. (BAS-2-32) Dictionary primary followed by a two digits search
40. (BAS-2-33) Dictionary primary preceded by a two digits search
41. (BAS-2-31) Dictionary primary preceded and followed by a one digit search
42. (BAS-2-19) Dictionary with two characters upper cased search
43. (BAS-2-43) Nine Markov characters with a threshold of one hundred search
44. (ADV-1-10) Two digits followed by three language-specific characters search
45. (ADV-1-11) Three language-specific characters followed by a two digit search
46. (ADV-1-04) All four-character, language-specific search
47. (BAS-3-01) Dictionary primary with a non-alphanumeric symbol inserted search
48. (BAS-3-04) Dictionary primary followed by a three digit search
49. (BAS-3-05) Dictionary primary preceded by a three digit search
50. (BAS-3-06) Social Security Number Search
51. (ADV-1-18) Three language-specific characters followed by a three digit search
52. (ADV-1-08) One digit followed by four language-specific characters search
53. (ADV-1-12) Four language-specific characters followed by a one digit search
54. (ADV-1-20) Dictionary primary followed by a two letter, language specific search
55. (ADV-1-21) Dictionary primary preceded by a two letter, language specific search
56. (ADV-1-15) Six letter, language specific search
57. English Transitional
58. English Transitional follows the same order of the DNA 3.1 and PRTK 6.1 English profile. It is useful for re-submitting unfinished jobs.

ARABIC

The Arabic profile begins by searching for simple passwords, followed by, dictionary and permutated dictionary searches, and ends with complex searches for dictionary and computed password. All default Arabic dictionaries and character sets are used.

DICTIONARIES

TABLE B-7 Default Dictionaries for the Arabic Profile

Dictionary Name	Dictionary Name
[AR-1] Names-ar-c.adf	[AR-2] Quran-ar-u.adf
[AR-1] Names-ar-u.adf	[AR-3] General-ar-c.adf
[AR-2] Quran-ar-c.adf	[AR-3] General-ar-u.adf

RULES (IN DEFAULT ORDER)

1. (BAS-1-01) One digit search
2. (BAS-1-03) Two digit search
3. (BAS-1-05) Three digit search
4. (BAS-1-07) Four digit search
5. (BAS-1-08) Five digit search
6. (BAS-1-02) One letter, language specific search
7. (BAS-1-04) Two letter, language specific search
8. (BAS-1-06) Three letter, language specific search
9. (ADV-1-01) All one-character, language-specific search
10. (ADV-1-02) All two character, language-specific search
11. (BAS-1-11) Four Markov characters with a threshold of one primary search
12. (BAS-2-03) Five Markov characters with a threshold of one primary search
13. (BAS-2-17) Dictionary primary search
14. (BAS-2-01) Four letter, language specific search
15. (BAS-2-04) Five Markov characters with a threshold of one primary reverse search
16. (ADV-1-07) One language-specific character followed by a four digit search
17. (BAS-1-10) Six digit search
18. (BAS-2-36) Date Search (two digit year)
19. (ADV-1-03) All three-character, language-specific search
20. BAS-2-18) Dictionary primary reverse search
21. (BAS-2-05) Six Markov characters with a threshold of one primary search
22. (BAS-2-07) Six Markov characters with a threshold of one primary reverse search
23. (BAS-2-09) Seven Markov characters with a threshold of fifty primary search
24. (BAS-2-21) Dictionary primary followed by common postfixes search
25. (BAS-2-22) Dictionary primary preceded by common prefixes search

26. (BAS-2-23) Dictionary primary followed by a one digit search
27. (BAS-2-24) Dictionary primary preceded by a one digit search
28. (BAS-2-25) Dictionary primary followed by a one letter, language specific search
29. (BAS-2-26) Dictionary primary preceded by a one letter, language specific search
30. (BAS-2-20) Dictionary primary character replacements search
31. (BAS-2-13) Eight digit search
32. (BAS-2-12) 7-digit telephone number search
33. (ADV-1-05) One digit followed by three language-specific characters search
34. (BAS-2-10) Seven Markov characters with a threshold of fifty primary reverse search
35. (BAS-2-02) Five letter, language specific search
36. (ADV-1-17) Two language-specific characters followed by four digits search
37. (BAS-2-14) Eight Markov characters with a threshold of fifty primary search
38. (BAS-2-15) Eight Markov characters with a threshold of fifty primary reverse search
39. (BAS-2-27) Dictionary primary followed by a non-alphanumeric symbol search
40. (BAS-2-28) Dictionary primary preceded by a language-specific non-alphanumeric symbol search
41. (BAS-2-32) Dictionary primary followed by a two digits search
42. (BAS-2-33) Dictionary primary preceded by a two digits search
43. (BAS-2-31) Dictionary primary preceded and followed by a one digit search
44. (BAS-2-19) Dictionary with two characters upper cased search
45. (ADV-1-10) Two digits followed by three language-specific characters search
46. (ADV-1-11) Three language-specific characters followed by a two digit search
47. (ADV-1-04) All four-character, language-specific search
48. (BAS-3-04) Dictionary primary followed by a three digit search
49. (BAS-3-05) Dictionary primary preceded by a three digit search
50. (BAS-3-06) Social Security Number Search
51. (ADV-1-18) Three language-specific characters followed by a three digit search
52. (ADV-1-08) One digit followed by four language-specific characters search
53. (ADV-1-12) Four language-specific characters followed by a one digit search
54. (ADV-1-20) Dictionary primary followed by a two letter, language specific search
55. (ADV-1-21) Dictionary primary preceded by a two letter, language specific search
56. (ADV-1-15) Six letter, language specific search

EUROPEAN

The European profile begins by searching for simple passwords, followed by dictionary and permutated dictionary searches, and ends with complex searches for dictionary and computed password. All default German, French, Italian, and Spanish dictionaries and character sets are used.

DICTIONARIES

TABLE B-8 Default Dictionaries for the European Profile

[DE-1] General-1-de-c.adf	[DE-1] General-4-de-u.adf
[DE-1] General-1-de-u.adf	[ES-1] General-es-c.adf
[DE-1] General-2-de-c.adf	[ES-1] General-es-u.adf
[DE-1] General-2-de-u.adf	[FR-1] General-fr-c.adf
[DE-1] General-3-de-c.adf	[FR-1] General-fr-u.adf
[DE-1] General-3-de-u.adf	[IT-1] General-it-c.adf
[DE-1] General-4-de-c.adf	[IT-1] General-it-u.adf

RULES (IN DEFAULT ORDER)

1. (BAS-1-01) One digit search
2. (BAS-1-03) Two digit search
3. (BAS-1-05) Three digit search
4. (BAS-1-07) Four digit search
5. (BAS-1-08) Five digit search
6. (BAS-1-02) One letter, language specific search
7. (BAS-1-04) Two letter, language specific search
8. (BAS-1-06) Three letter, language specific search
9. (ADV-1-01) All one-character, language-specific search
10. (ADV-1-02) All two character, language-specific search
11. (BAS-1-11) Four Markov characters with a threshold of one primary search
12. (BAS-2-03) Five Markov characters with a threshold of one primary search
13. (BAS-2-17) Dictionary primary search
14. (BAS-2-01) Four letter, language specific search
15. (BAS-2-04) Five Markov characters with a threshold of one primary reverse search

16. (ADV-1-07) One language-specific character followed by a four digit search
17. (BAS-1-10) Six digit search
18. (BAS-2-36) Date Search (two digit year)
19. (ADV-1-03) All three-character, language-specific search
20. (BAS-2-18) Dictionary primary reverse search
21. (BAS-2-05) Six Markov characters with a threshold of one primary search
22. (BAS-2-07) Six Markov characters with a threshold of one primary reverse search
23. (BAS-2-09) Seven Markov characters with a threshold of fifty primary search
24. (BAS-2-21) Dictionary primary followed by common postfixes search
25. (BAS-2-22) Dictionary primary preceded by common prefixes search
26. (BAS-2-23) Dictionary primary followed by a one digit search
27. (BAS-2-24) Dictionary primary preceded by a one digit search
28. (BAS-2-25) Dictionary primary followed by a one letter, language specific search
29. (BAS-2-26) Dictionary primary preceded by a one letter, language specific search
30. (BAS-2-20) Dictionary primary character replacements search
31. (BAS-2-13) Eight digit search
32. (BAS-2-12) Seven digit telephone number search
33. (ADV-1-05) One digit followed by three language-specific characters search
34. (BAS-2-10) Seven Markov characters with a threshold of fifty primary reverse search
35. (BAS-2-02) Five letter, language specific search
36. (ADV-1-17) Two language-specific characters followed by four digits search
37. (BAS-2-14) Eight Markov characters with a threshold of fifty primary search
38. (BAS-2-15) Eight Markov characters with a threshold of fifty primary reverse search
39. (BAS-2-27) Dictionary primary followed by a non-alphanumeric symbol search
40. (BAS-2-28) Dictionary primary preceded by a language-specific non-alphanumeric symbol search
41. (BAS-2-32) Dictionary primary followed by a two digits search
42. (BAS-2-33) Dictionary primary preceded by a two digits search
43. (BAS-2-31) Dictionary primary preceded and followed by a one digit search
44. (BAS-2-19) Dictionary with two characters upper cased search
45. (ADV-1-10) Two digits followed by three language-specific characters search
46. (ADV-1-11) Three language-specific characters followed by a two digit search
47. (ADV-1-04) All four-character, language-specific search

48. (BAS-3-04) Dictionary primary followed by a three digit search
49. (BAS-3-05) Dictionary primary preceded by a three digit search
50. (BAS-3-06) Social Security Number Search
51. (ADV-1-18) Three language-specific characters followed by a three digit search
52. (ADV-1-08) One digit followed by four language-specific characters search
53. (ADV-1-12) Four language-specific characters followed by a one digit search
54. (ADV-1-20) Dictionary primary followed by a two letter, language specific search
55. (ADV-1-21) Dictionary primary preceded by a two letter, language specific search
56. (ADV-1-15) Six letter, language specific search

RUSSIAN

The Russian profile begins by searching for simple passwords, followed by, dictionary and permutated dictionary searches, and ends with complex searches for dictionary and computed password. All default Russian dictionaries and character sets are used.

DICTIONARIES

TABLE B-9 Default Dictionaries for the Default Russian Profile

Dictionary Name	Dictionary Name
[RU-1] General-1-ru-c.adf	[RU-1] General-2-ru-c.adf
[RU-1] General-1-ru-u.adf	[RU-1] General-2-ru-u.adf

RULES (IN DEFAULT ORDER)

1. (BAS-1-01) One digit search
2. (BAS-1-03) Two digit search
3. (BAS-1-05) Three digit search
4. (BAS-1-07) Four digit search
5. (BAS-1-08) Five digit search
6. (BAS-1-02) One letter, language specific search
7. (BAS-1-04) Two letter, language specific search
8. (BAS-1-06) Three letter, language specific search
9. (ADV-1-01) All one-character, language-specific search
10. (ADV-1-02) All two character, language-specific search
11. (BAS-1-11) Four Markov characters with a threshold of one primary search

12. (BAS-2-03) Five Markov characters with a threshold of one primary search
13. (BAS-2-17) Dictionary primary search
14. (BAS-2-01) Four letter, language specific search
15. (BAS-2-04) Five Markov characters with a threshold of one primary reverse search
16. (ADV-1-07) One language-specific character followed by a four digit search
17. (BAS-1-10) Six digit search
18. (BAS-2-36) Date Search (Two digit year)
19. (ADV-1-03) All three-character, language-specific search
20. (BAS-2-18) Dictionary primary reverse search
21. (BAS-2-05) Six Markov characters with a threshold of one primary search
22. (BAS-2-07) Six Markov characters with a threshold of one primary reverse search
23. (BAS-2-09) Seven Markov characters with a threshold of fifty primary search
24. (BAS-2-21) Dictionary primary followed by common postfixes search
25. (BAS-2-22) Dictionary primary preceded by common prefixes search
26. (BAS-2-23) Dictionary primary followed by a one digit search
27. (BAS-2-24) Dictionary primary preceded by a one digit search
28. (BAS-2-25) Dictionary primary followed by a one letter, language specific search
29. (BAS-2-26) Dictionary primary preceded by a one letter, language specific search
30. (BAS-2-20) Dictionary primary character replacements search
31. (BAS-2-13) Eight digit search
32. (BAS-2-12) Seven digit telephone number search
33. (ADV-1-05) One digit followed by three language-specific characters search
34. (BAS-2-10) Seven Markov characters with a threshold of fifty primary reverse search
35. (BAS-2-02) Five letter, language specific search
36. (ADV-1-17) Two language-specific characters followed by four digits search
37. (BAS-2-14) Eight Markov characters with a threshold of fifty primary search
38. (BAS-2-15) Eight Markov characters with a threshold of fifty primary reverse search
39. (BAS-2-27) Dictionary primary followed by a non-alphanumeric symbol search
40. (BAS-2-28) Dictionary primary preceded by a language-specific non-alphanumeric symbol search
41. (BAS-2-32) Dictionary primary followed by a two digits search
42. (BAS-2-33) Dictionary primary preceded by a two digits search
43. (BAS-2-31) Dictionary primary preceded and followed by a one digit search

44. (BAS-2-19) Dictionary with two characters upper cased search
45. (ADV-1-10) Two digits followed by three language-specific characters search
46. (ADV-1-11) Three language-specific characters followed by a two digit search
47. (ADV-1-04) All four-character, language-specific search
48. (BAS-3-04) Dictionary primary followed by a three digit search
49. (BAS-3-05) Dictionary primary preceded by a three digit search
50. (BAS-3-06) Social Security Number Search
51. (ADV-1-18) Three language-specific characters followed by a three digit search
52. (ADV-1-08) One digit followed by four language-specific characters search
53. (ADV-1-12) Four language-specific characters followed by a one digit search
54. (ADV-1-20) Dictionary primary followed by a two letter, language specific search
55. (ADV-1-21) Dictionary primary preceded by a two letter, language specific search
56. (ADV-1-15) Six letter, language specific search

PASS-PHRASE

All Pass-phrase Rules are in English

DICTIONARIES

TABLE B-10 Default Dictionaries for the Default Pass-Phrase Profile

Dictionary Name	Dictionary Name
[EN-1] Common-en-c.adf	[EN-3] Names-en-u.adf
[EN-1] Common-en-u.adf	[EN-4] General-1-en-c.adf
[EN-2] Miscellaneous-en-c.adf	[EN-4] General-1-en-u.adf
[EN-2] Miscellaneous-en-u.adf	[EN-4] General-2-en-c.adf
[EN-3] Names-en-c.adf	[EN-4] General-2-en-u.adf

RULES (IN DEFAULT ORDER)

1. (PP-1-03) Dictionary preceded by a verb or prepositional phrase search
2. (PP-1-04) The common English dictionary preceded by a verb or prepositional phrase search
3. (PP-2-01) Word inserted into another word search

4. (PP-2-02) Dictionary followed by a verb or prepositional phrase followed by a Dictionary search
5. (PP-2-03) Two word pass-phrase using the common English dictionary
6. (PP-3-01) Three word concatenation without spaces search
7. (PP-3-02) Three word concatenation with spaces search
8. (PP-3-03) Four word concatenation without spaces search
9. (PP-3-04) Four word concatenation with spaces search

FTK IMPORT

Used as a template for FTK imported word lists.

DICTIONARIES

None Defined. Intended for user to select FTK imported dictionaries.

RULES

Dictionary normalized, lowercase search.

PRTK

Rules in this profile are ordered by research conducted on recovered passwords.

DICTIONARIES

TABLE B-11 Default Dictionaries for the Default PRTK Profile

Dictionary Name	Dictionary Name
[EN-1] Common-en-c.adf	[EN-3] Names-en-u.adf
[EN-1] Common-en-u.adf	[EN-4] General-1-en-c.adf
[EN-2] Miscellaneous-en-c.adf	[EN-4] General-1-en-u.adf
[EN-2] Miscellaneous-en-u.adf	[EN-4] General-2-en-c.adf
[EN-3] Names-en-c.adf	[EN-4] General-2-en-u.adf

RULES (IN DEFAULT ORDER)

1. (BAS-1-01) One digit search

2. (BAS-1-07) Four digit search
3. (BAS-1-03) Two digit search
4. (BAS-2-17) Dictionary primary search
5. (BAS-1-02) One letter, language specific search
6. (BAS-1-05) Three digit search
7. (ADV-1-01) All one-character, language-specific search
8. (BAS-1-04) Two letter, language specific search
9. (BAS-2-23) Dictionary primary followed by a one digit search
10. (BAS-1-08) Five digit search
11. (ADV-1-02) All two character, language-specific search
12. (BAS-1-06) Three letter, language specific search
13. (BAS-1-10) Six digit search
14. (BAS-2-01) Four letter, language specific search
15. (ADV-1-03) All three-character, language-specific search
16. (BAS-2-25) Dictionary primary followed by a one letter, language specific search
17. (BAS-2-08) Seven digit search
18. (ADV-1-04) All four-character, language-specific search
19. (ADV-1-09) Two language-specific characters followed by a three digit search
20. (BAS-2-20) Dictionary primary character replacements search
21. (BAS-2-03) Five Markov characters with a threshold of one primary search
22. (BAS-2-13) Eight digit search
23. (BAS-2-02) Five letter, language specific search
24. (BAS-2-32) Dictionary primary followed by a two digits search
25. (ADV-1-20) Dictionary primary followed by a two letter, language specific search
26. (BAS-2-09) Seven Markov characters with a threshold of fifty primary search
27. (ADV-1-07) One language-specific character followed by a four digit search
28. (BAS-2-26) Dictionary primary preceded by a one letter, language specific search
29. (BAS-2-18) Dictionary primary reverse search
30. (ADV-1-05) One digit followed by three language-specific characters search
31. (ADV-1-15) Six letter, language specific search
32. (ADV-2-01) All five-character, language-specific search

DNA

Rules in this profile are ordered by research conducted on recovered passwords.

DICTIONARIES

TABLE B-12 Default Dictionaries for the Default DNA Profile

Dictionary Name	Dictionary Name
[EN-1] Common-en-c.adf	[EN-3] Names-en-u.adf
[EN-1] Common-en-u.adf	[EN-4] General-1-en-c.adf
[EN-2] Miscellaneous-en-c.adf	[EN-4] General-1-en-u.adf
[EN-2] Miscellaneous-en-u.adf	[EN-4] General-2-en-c.adf
[EN-3] Names-en-c.adf	[EN-4] General-2-en-u.adf

RULES (IN DEFAULT ORDER)

1. (BAS-1-01) One digit search
2. (BAS-1-07) Four digit search
3. (BAS-1-03) Two digit search
4. (BAS-2-17) Dictionary primary search
5. (BAS-1-02) One letter, language specific search
6. (BAS-1-05) Three digit search
7. (ADV-1-01) All one-character, language-specific search
8. (BAS-1-04) Two letter, language specific search
9. (BAS-2-23) Dictionary primary followed by a one digit search
10. (BAS-1-08) Five digit search
11. (ADV-1-02) All two character, language-specific search
12. (BAS-1-06) Three letter, language specific search
13. (BAS-1-10) Six digit search
14. (BAS-2-01) Four letter, language specific search
15. (ADV-1-03) All three-character, language-specific search
16. (BAS-2-25) Dictionary primary followed by a one letter, language specific search
17. (BAS-2-08) Seven digit search
18. (ADV-1-04) All four-character, language-specific search
19. (ADV-1-09) Two language-specific characters followed by a three digit search

20. (BAS-2-20) Dictionary primary character replacements search
21. (BAS-2-03) Five Markov characters with a threshold of one primary search
22. (BAS-2-13) Eight digit search
23. (BAS-2-02) Five letter, language specific search
24. (BAS-2-32) Dictionary primary followed by a two digits search
25. (ADV-1-20) Dictionary primary followed by a two letter, language specific search
26. (BAS-2-09) Seven Markov characters with a threshold of fifty primary search
27. (ADV-1-07) One language-specific character followed by a four digit search
28. (BAS-2-26) Dictionary primary preceded by a one letter, language specific search
29. (BAS-2-18) Dictionary primary reverse search

CHARACTER REPLACEMENTS

This list shows characters commonly replaced for each other:

TABLE B-13 PRTK and DNA Common Character Replacements

Replace 1 with L	Replace e with 3	Replace l with |
Replace 1 with i	Replace e with [	Replace l with !
Replace 3 with]	Replace e with {	Replace L with 1
Replace 3 with }	Replace f with ph	Replace o with 0
Replace a with @	Replace g with @	Replace o with ()
Replace a with 4	Replace h with 4	Replace ph with f
Replace a with 2	Replace i with !	Replace s with 5
Replace b with 3	Replace i with 1	Replace s with $
Replace c with (	Replace i with][	Replace z with 5
Replace e with 3	Replace i with |	

COMMON PREFIXES

The following is a list of common prefixes known to PRTK and DNA.

TABLE B-14 PRTK and DNA Common Prefixes

123	!@#	2u	de	con	net	pro
abc	4u	dr	in	dis	non	sub
mr	4u2	re	un	mac	out	anti

TABLE B-14 PRTK and DNA Common Prefixes

mrs	2b	co	bio	mis	pre	non-
over	poly	post	semi	tele	#1	

COMMON SUFFIXES (A.K.A. POSTFIXES)

The following is a list of common suffixes.

TABLE B-15 PRTK and DNA Common Suffixes

#1	dr	s	ly	ers
123	!@#	‘s	er	ity
abc	4u	es	ing	ness
mr	4u2	ed	ies	ites
mrs	2b	en	ism	isms

PREPOSITIONAL AND VERB PHRASES

The following is a list of phrases known to PRTK and DNA

TABLE B-16 PRTK and DNA Known Prepositional Phrases

in	in the	into the	is a	is the
was a	was the	has a	has the	had a
for a	for the	of a	of the	with a
going to	going to the	is in the	should be	would be
and	not	could	can	had the
with the				

Appendix C
Encryption Technology

To understand how Password Recovery Toolkit® (PRTK®) 6.5 and Distributed Network Attack (DNA®) 3.5 search for the different password combinations available for application files, you need to be familiar with the underlying elements and classifications of encryption and password technology.

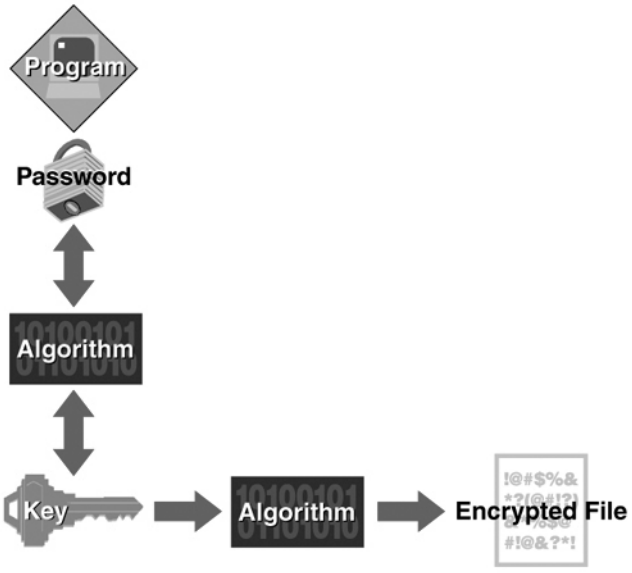
UNDERSTANDING ENCRYPTED FILES

An encrypted file is digitally altered so the file's data cannot be read without the key. In a binary editor, the data within an encrypted file appears as unintelligible characters. The only way to access an encrypted file is to open the file in its native application using the file's password.

When you password protect and encrypt a file, the program you are using applies an algorithm to the password to create a digital key which is used to lock the file. This is the first line of defense. The program then uses the key and a different algorithm to encrypt the file. The file is locked and encrypted so both the file and its data are protected. To access the file, you must open the file in its native program and enter a

password that produces the identical key. The program uses the key and a reverse algorithm to decrypt the file.

Figure C-1 Understanding the File Encryption Process



UNDERSTANDING THE PRTK & DNA DECRYPTION PROCESS

To recover an encrypted document, you need a password or a "key," a long series of binary data.

Typically applications use a transformation function that allows a user to enter a password to encrypt or decrypt a file. So, if you create an encrypted document in Microsoft Word, you only use a password. Microsoft Word then transforms that password into a key, without you even knowing it. The same password generates the same key every time.

To obtain either a password or a key, PRTK uses the following attack types. Each attack type is discussed in more detail in the following sections.

- **Decryption Attack**: Decrypts the password that locks the file.
- **Dictionary Attack**: Uses the words in a dictionary, applies Rules to the words, and converts the possible words into keys.

- **Keyspace Attack:** Tries every possible key because there is a finite number of keys for the file.
- The possible number of keys can be very large, but with enough computing power, it is possible to try every key.
- **Reset**: Rewrites the key that opens the file to a key that comes from a password that you specify.

DECRYPTION ATTACK

The decryption attack looks for the password that locks the file. In the files that PRTK uses the decryption attack on, the password is protected or scrambled with a known key. The password is then stored in the file itself.

PRTK knows the key that encrypts the password because the application uses the same key each time. (Each application in the decryption attack category uses a different key.) PRTK knows the location of the encrypted password in the file, applies the key to it, and then decrypts the password.

DICTIONARY ATTACK

PRTK tries to find the passwords of these documents, because an exhaustive key search takes an unreasonable amount of time.

Most people use passwords that they can remember. If you limit a set of passwords to a language they speak or other biographical data of the people, there is a good chance of finding the password in a reasonable time frame.

The language, biographical data, and other information is stored in dictionaries. PRTK uses dictionaries to try to find a password. Rules are applied to the words in a dictionary to further attempt password recovery.

For example, one Rule is a primary search using the dictionaries. The primary search includes the words with all lower-case letters, all capital letters, one capital letter followed by all lower-case letters, and one lower-case letter followed by all capital letters, such as hello, Hello, HELLO, hELLO etc.

When PRTK discovers a password, it adds it automatically to a Golden Dictionary. Each time a new password is added, the updated Golden Dictionary is applied to the

jobs in the job queue. If there are jobs with duplicate passwords, PRTK automatically discovers them by using the Golden Dictionary.

KEYSPACE ATTACK

The keyspace attack is typically used on applications that use 40-bit encryption or less. In 32-bit encryption applications, such as WinZip 6.0–8.1, there is a limit to the number of keys that can be stored. The limit is the largest number that can be represented with 32 bits.

This number might seem extremely large; but it is actually small enough that, with enough computing power, you can decrypt an encrypted document in a reasonable amount of time.

So with certain applications, PRTK generally finds the key for an encrypted document rather than the password because there are a relatively small number of keys that can be created, and key recovery is guaranteed.

RESET ATTACK

In the reset attack, two types of keys are associated with an encrypted file: one key that encrypts the password for the file and one key that actually encrypts the file. The reset attack usually rewrites the key that encrypts the file to a key that comes from a known password.

CURRENT ENCRYPTION STANDARDS

Although it is helpful to understand the methods by which documents are encrypted, PRTK actually deciphers this information for you when you recover a password and does not require any user input.

SYMMETRIC ENCRYPTION

In *symmetric encryption*, the encryption and decryption keys are the same. Some common symmetric encryption systems are:

- Data Encryption Standard (DES) is a 56-bit standard that is considered weak by current standards. It can easily be broken by a special hardware device known as

"deep crack," and it can be broken with a distributed network of computers. Triple-DES (3DES) can be used with two keys (EDE2 112-bit) or three keys (EDE3 168-bit).

- Pretty Good Privacy (PGP) is used for sending secure email. It provides both confidentiality and authentication.
- BestCrypt can be used with any of the following Hash functions and encryption algorithms: GOST and SHA Hash; GOST, DES, Blowfish, IDEA, Twofish, CAST, AES, RC6, and 3DES encryption.
- Advanced Encryption Standard (AES) has replaced DES as the encryption standard. It uses a 128-, 192-, or 256-bit key.

RC4

RC4 is a variable key-length stream cipher designed by RSA. Microsoft Word and Excel use RC4 and a 40-bit key to encrypt their files. Keys this small can be easily broken by governments, criminals, and amateurs.

ASYMMETRIC ENCRYPTION

In *asymmetric encryption*, the encryption and decryption keys are different. Asymmetric encryption uses a public key (which can be posted on an Internet site or made "public" through other means) and a private key, which remains secret.

In this system, something that has been encrypted with the private key can only be decrypted by the public key, and vice versa.

Asymmetric algorithms are slower than symmetric algorithms, but can nonetheless be very useful. They are often used in combination with symmetric algorithms.

The number of possible key values refers to the actual number of different key words or passwords that can exist, based on the particular algorithm used to create the key value in question. This number can be calculated as follows: an *n*-bit key has 2^n possible values. For example, a 40-bit key has 2^{40} possible values, or approximately one trillion possibilities.

The security of an algorithm should rely on the secrecy of the key only, not the secrecy of the algorithm.

HASHING

Hashing is used to determine whether a file has changed. Producing two different items with the same hash value is computationally improbable since changing a single bit in a file results in a completely different hash. Therefore, hashes can function as a type of digital fingerprint that can be used to verify data integrity.

Before PRTK begins a password recovery, it automatically creates SHA and MD5 hash values for the files to be recovered. After a password is recovered, you can verify the hash values of a file providing proof that the contents of the file were not changed during the recovery of the file's password.

PRTK uses two different hashing methods.

SECURE HASH ALGORITHM (SHA)

The National Institute of Standards and Technology (NIST) designed the Secure Hash Algorithm (SHA). SHA takes as input an arbitrary-length file and outputs a fixed-length number referred to as a "hash" or "digest." SHA-1 produces a 160-bit (20 byte) digest. SHA hashes take longer to generate than MD5 hashes.

MESSAGE DIGEST 5 (MD5)

Message Digest 5 (MD5) was developed by Professor Ronald L. Rivest. MD5 takes as input an arbitrary-length file and outputs a fixed-length number referred to as a "hash" or "digest." MD5 produces a 128-bit (16-byte) digest. MD5 is a faster implementation than SHA.

Appendix D
Program Files

This chapter identifies key program files, their locations, and their functions for Password Recovery Toolkit® (PRTK®) 6.5 and for Distributed Network Attack® (DNA®)3.5.

PRTK FILES

The following table details the filenames, their default locations, and their functions in a PRTK system.

TABLE D-1 PRTK Paths, Filenames, and Functions

Filename	Directory Location	Function
*.adf	[drive]:\documents and settings\all users\ application data\ AccessData\PR\ Dictionaries	A dictionary file. Codepage dictionaries have -c appended to the filename. Unicode dictionaries have -u appended to the filename. When a Biographical Dictionary is generated, three files are created, the two *.adf files, and one .xml file. The .xml file contents cannot be viewed as the .adf files can. A Biographical Dictionary preserves the case of alpha characters.

TABLE D-1 PRTK Paths, Filenames, and Functions

Filename	Directory Location	Function
*.profile	[drive]:\documents and settings\all users\ application data\ AccessData\PR\ Profiles	A profile file, which contains information about the dictionaries and Rules used to decrypt files.
\bin directory	[drive]:\Program Files\AccessData\PRTK 6\ Supervisor\bin	A directory containing a portion of the Java Runtime Environment, which runs PRTK.
\data directory	[drive]:\Documents and Settings\All Users\ Application Data\ AccessData\PR\dnadata	The directory that contains the PRTK database files.
\Dictionaries directory	[drive]:\documents and settings\all users\ application data\ AccessData\PR\ Dictionaries	The directory that contains the dictionaries used by PRTK.
GoldenDictionary	[drive]:\documents and settings\all users\ application data\ AccessData\PR\ Dictionaries	A file added after the installation that contains all passwords recovered by PRTK.
\Rules directory	[drive]:\documents and settings\all users\ application data\ AccessData\PR\levels	The directory that contains the password recovery Rules used by PRTK.
\lib directory	[drive]:\Program Files\AccessData\PRTK 6\ Supervisor\lib	A directory containing a portion of the Java Runtime Environment, which runs PRTK.
\Modules directory	[drive]:\documents and settings\all users\ application data\ AccessData\PR\ Modules	The directory that contains the application modules supported by PRTK.

TABLE D-1 PRTK Paths, Filenames, and Functions

Filename	Directory Location	Function
\Profiles directory	[drive]:\documents and settings\all users\application data\AccessData\PR\ Profiles	The directory that contains the profiles used by PRTK.
ad_dictutility.jar	C:\Program Files\ AccessData\PRTK 6\ Supervisor	The Dictionary Utility program.

DNA SUPERVISOR FILES

The following table details the filenames, their default locations, and their functions in a DNA Supervisor.

TABLE D-2 DNA Supervisor Paths, Filenames, and Functions

Filename	Directory Location	Function
*.adf	[Drive]:\Documents and Settings\All Users\ Application Data\ AccessData\PR\dictionaries	A dictionary file. Codepage dictionaries have -c appended to the filename. Unicode dictionaries have -u appended to the filename. When a Biographical Dictionary is generated, three files are created, the two .adf files, and one .xml file. The .xml file contents cannot be viewed as the .adf files can. A Biographical Dictionary preserves the case of alpha characters.
*.profile	[Drive]:\Documents and Settings\All Users\ Application Data\ AccessData\PR\profiles	A profile file, which contains information about the dictionaries and Rules used to decrypt files.
\bin directory	[Drive]:\Program Files\ AccessData\DNA 3\ Supervisor\bin	A directory used by the Java Virtual Machine, which runs DNA.

TABLE D-2 DNA Supervisor Paths, Filenames, and Functions

Filename	Directory Location	Function
\data directory	[Drive]:\Documents and Settings\All Users\ Application Data\ AccessData\PR\dnadata	The directory that contains the DNA database files.
\Dictionaries directory	[Drive]:\Documents and Settings\All Users\ Application Data\ AccessData\PR\dictionaries	The directory that contains the dictionaries used by DNA.
generate_keys.exe	[Drive]:\Program Files\ AccessData\DNA 3\ Supervisor	A file used by the DNA installation program to create encrypted communication between the supervisor and worker.
generate_worker_ install.exe	[Drive]:\Program Files\ AccessData\DNA 3\ Supervisor	A file used by the DNA installation program to create the DNA Worker installation files available in the Supervisor directory.
GoldenDictionary	[Drive]:\Documents and Settings\All Users\ Application Data\ AccessData\PR\dictionaries	A file added after the installation that contains all passwords recovered by the DNA Supervisor.
\Rules directory	[Drive]:\Documents and Settings\All Users\ Application Data\ AccessData\PR\levels	The directory that contains the password recovery Rules used by DNA.
\lib directory	[Drive]:\Program Files\ AccessData\DNA 3\ Supervisor\lib	A directory used by the Java Virtual Machine, which runs DNA.
\Modules directory	[Drive]:\Documents and Settings\All Users\ Application Data\ AccessData\PR\Modules	The directory that contains the application modules supported by DNA.
\Profiles directory	[Drive]:\Documents and Settings\All Users\ Application Data\ AccessData\PR\profiles	The directory that contains the profiles used by DNA.

TABLE D-2 DNA Supervisor Paths, Filenames, and Functions

Filename	Directory Location	Function
prefs.dat	[Drive]:\Documents and Settings\All Users\ Application Data\ AccessData\PR	A file added after the installation that holds preferences, including the option to decrypt the file after key recovery and the dimensions of the DNA management interface.
Supervisor_service.exe and Supervisor.ini	[Drive]:\Program Files\ AccessData\DNA 3\ Supervisor	The DNA Supervisor program. You manage the DNA Supervisor from the management interface. The Supervisor.ini file is where the keys are stored.
user_defined.xml	[Drive]:\Documents and Settings\All Users\ Application Data\ AccessData\PR\levels	The file that contains information about each Rule that you have created.
worker.ini	[Drive]:\Documents and Settings\All Users\ Application Data\ AccessData\PR	The DNA Worker program. This file is only added to this directory if the DNA Worker is installed on the same machine as the supervisor.
worker-i386-install.sh	[Drive]:\Program Files\ AccessData\DNA 3\ Supervisor	The DNA Worker installation program for Linux machines.
worker_service.exe	[Drive]:\Program Files\ AccessData\DNA 3\ Supervisor	A file used by the DNA installation program to create the services needed by the DNA Worker installation files available in the Supervisor directory.
worker-mac-install.sh	[Drive]:\Program Files\ AccessData\DNA 3\ Supervisor	The DNA Worker installation program for Macintosh machines.
worker-powerpc-install.sh	[Drive]:\Program Files\ AccessData\DNA 3\ Supervisor	The DNA Worker installation program for PowerPC machines.

DNA WORKER FILES

The following table details the filenames, their default locations, and their functions in a DNA Worker.

TABLE D-3 DNA Worker Paths, Filenames, and Functions

Filename	Directory Location	Function
*.adf	C:\Documents and Settings\All Users\ Application Data\ AccessData\PR\ dictionaries	A dictionary file that the worker receives from the supervisor when it processes jobs. Codepage dictionaries have -c appended to the filename. Unicode dictionaries have -u appended to the filename.
\bin directory	C:\Program Files\ AccessData\DNA 3\ Worker\bin	A directory used by the Java Virtual Machine, which runs DNA Worker.
\lib directory	C:\Program Files\ AccessData\DNA 3\ Worker\lib	A directory used by the Java Virtual Machine, which runs DNA Worker.
worker.exe	C:\Program Files\ AccessData\DNA 3\ Worker	The DNA Worker User Interface program. On the DNA Worker machine, you can check statistics as they are updated, and you can stop and restart the worker from the DNA Worker interface.
Worker.ini	C:\Documents and Settings\All Users\ Application Data\ AccessData\PR	The file that contains configuration information about the worker, including its supervisor hostname and IP address.
worker_service.exe	C:\Program Files\ AccessData\DNA 3\ Worker	A service needed by the DNA Worker. This service must be running in order to process jobs on the DNA Worker.
ad_dictutility.jar	C:\Program Files\ AccessData\DNA 3\ Supervisor	The Dictionary Utility program.

Appendix E
Recovering EFS Files

On Windows 2000 and Windows XP systems, Microsoft's encrypted file system (EFS) allows you to encrypt a single file or to automatically encrypt all files saved to a particular folder. You don't have to remember passwords because Windows encrypts the data using your login password.

You must use FTK to decrypt EFS-encrypted files to get the SYSKEY. PRTK recovers EFS files by retrieving your login password from the EFS master key file ([*drive*]:\Documents and Settings\user\Application Data\Protect\user_SID).

Ultimately, this recovery performs the same function as the SAM file attack. Recovering the user login password from the SAM file can be faster than recovering the login password from the EFS master key file. Use the SAM file to recover the user's login password.

Note: When used in conjunction with PRTK, FTK1.50b and above has an option to automatically decrypt EFS files. Essentially, FTK sends PRTK the EFS master key file along with any other EFS-related keys. PRTK then performs an EFS attack to obtain the user login password. FTK and PRTK must be running on the same dongle on the same machine to support this integrated functionality.

RECOVERING EFS ON WINDOWS XP SERVICE PACK 1 OR LATER

If you are using Windows XP Service Pack 1 or later, you must export the SAM and SYSTEM file using FTK Imager or FTK and import the files into PRTK to obtain the login password. After PRTK has obtained the password, you can provide the password to FTK so that FTK can continue decrypting the EFS files.

To recover EFS files:

1. Start PRTK.
2. In PRTK, add the SAM file and browse to the SYSTEM file when the syskey is requested.
3. After obtaining the login password, start FTK.
4. In FTK, select *Tools* > *Enter EFS Password.*
5. Click *OK.*
6. Enter the password.

FTK decrypts the EFS passwords if the login password obtained from the SAM and SYSTEM files is valid. If FTK cannot decrypt the EFS passwords, either the login password has been changed after the SAM and SYSTEM files were obtained or the EFS file was encrypted by another user.

Important: If there are multiple users on a workstation, you must have all user login passwords to increase chances of decrypting the files. EFS files could have been encrypted by more than one of the users. FTK and PRTK must be running on the same dongle on the same machine to support this integrated functionality.

OTHER NOTES

In Windows 2000, every file is also encrypted with the Recovery Agent's EFS public key. The Administrator user is the default Recovery Agent for computers that are not a part of a domain. If the computer is joined to a Windows 2000 domain, the Domain Administrator user is the default Recovery Agent. In Windows XP, the Recovery Agent is optional.

Certain files cannot be encrypted:

- System files
- NTFS compressed files
- Files in %Systemroot% and its subdirectories

AccessData Glossary

A

AccessData Recovery Session

In PRTK, selecting one or more files and starting the password recovery process is called an AccessData Recovery (ADR) session. Typically, each case has one session unless you have a large number of encrypted files.

Address

A location of data, usually in main memory or on a disk. You can think of computer memory as an array of storage boxes, each of which is one byte in length. Each computer has an address (a unique number) assigned to it. By specifying a memory address, programmers can access a particular byte of data. Disks are divided into tracks and sectors, each of which has a unique address.

Advanced Encryption Standard

A common symmetric encryption system that has replaced Data Encryption Standard as the encryption standard. It uses a 128, 192, or 256-bit key.

Application Administrator

The first user created in an AccessData FTK2 system. The Application Administrator has all rights within the application, including adding users and assigning roles. Application Administrators can assign the role of Application Administrator to new users as they are created.

Asymmetric Encryption

A type of encryption in which the encryption and decryption keys are different. Asymmetric encryption uses a public key (which can be posted on an Internet site or made "public" through other means) and a private key, which remains secret. In this system, something that has been encrypted with the private key can be decrypted only by the public key, and vice versa. Asymmetric algorithms are slower than symmetric algorithms, but can nonetheless be very useful. They are often used in combination with symmetric algorithms, as with EFS Encryption.

The number of possible key values refers to the actual number of different key words or passwords that can exist, based on the particular algorithm used to create the key value in question. A n-bit key has 2n possible values. For example, a 40-bit key has 240 possible values, or 1,099,511,627,776 possibilities.

The security of an algorithm should rely on the secrecy of the key only, not the secrecy of the algorithm.

Do not compare key sizes between symmetric and asymmetric algorithms. For example, a 128-bit symmetric key is approximately as strong as a 512-bit asymmetric key.

B

BestCrypt

A common symmetric encryption system that can be used with any of the following hash functions and encryption algorithms:

- GOST
- SHA-1 Hash
- Blowfish
- IDEA
- Twofish
- CAST
- AES
- RC6
- 3DES encryption

Binary

Pertaining to a number system that has just two unique digits. Computers are based on the binary numbering system, which consists of just two unique numbers, 0 and 1. All operations that are possible in the decimal system (addition, subtraction, multiplication, and division) are equally possible in the binary system.

BIOS

Acronym for Basic Input/Output System. The BIOS is built-in software that determines what a computer can do without accessing programs from a disk. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions.

Bit-stream Image

See "Forensic Image" on page 238.

Bookmark

A menu entry or icon on a computer that is most often created by the user and that serves as a shortcut to a previously viewed location (as an Internet address). The term "bookmark" as used in a Computer Crimes Unit report refers to locating a file, folder or specific item of interest to the examiner or to the investigator. The location of the data (file name, file location, relative path, and hardware address) is identified. Other data can be addressed as well.

Boot

To load the first piece of software that starts a computer. Because the operating system is essential for running all other programs, it is usually the first piece of software loaded during the boot process.

Boot Record

All the three types of FAT have a boot record, which is located within an area of reserved sectors. The DOS format program reserves 1 sector for FAT12 and FAT16 and usually 32 sectors for FAT32.

C

Chunk Size

The number of passwords the supervisor machine can process in the amount of time specified.

Cluster

Fixed-length blocks that store files on the FAT media. Each cluster is assigned a unique number by the computer operating system. Only the part of the partition called the "data area" is divided into clusters. The remainder of the partition are defined as sectors. Files and directories store their data in these clusters. The size of one cluster is specified in a structure called the Boot Record, and can range from a single sector to 128 sectors. The operating system assigns a unique number to each cluster and the keeps track of files according to which cluster they use.

CMOS

Short for Complementary Metal Oxide Semiconductor. Pronounced SEE-moss, CMOS is a widely used type of semiconductor. CMOS semiconductors use both NMOS (negative polarity) and PMOS (positive polarity) circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor. This makes them particularly attractive for use in battery-powered devices, such as portable computers. Personal computers also contain a small amount of battery-powered CMOS memory to hold the date, time, and system setup parameters.

CRC

Short for Cyclical Redundancy Check. It performs a complex calculation on every byte in the file, generating a unique number for the file in question. If so much as a single byte in the file being checked were to change, the cyclical redundancy check value for that file would also change. If the CRC value is known for a file before it is downloaded, you can compare it with the CRC value generated by this software after the file has been downloaded to ascertain whether the file was damaged in transit. The odds of two files having the same CRC value are even longer than the odds of winning a state-run lottery—along the lines of one in 4,294,967,296.

Cylinder

A single-track location on all the platters making up a hard disk. For example, if a hard disk has four platters, each with 600 tracks, then there will be 600 cylinders, and each cylinder will consist of 8 tracks (assuming that each platter has tracks on both sides).

D

dd

(Linux) Makes a copy of a input file (STDIN) using the specified conditions, and sends the results to the output file (STDOUT).

Data Carving

Data carving is the process of extracting a collection of data from a larger data set. Data carving techniques frequently occur during a digital investigation when the unallocated file system space is analyzed to extract files. The files are "carved" from the unallocated space using file type-specific header and footer values. File system structures are not used during the process.

Data Encryption Standard

A 56-bit symmetric encryption system that is considered weak by current standards. It has been broken in a distributed environment.

Device

Any machine or component that attaches to a computer. Examples of devices include disk drives, printers, mice, and modems. These particular devices fall into the category of peripheral devices because they are separate from the main computer.

Most devices, whether peripheral or not, require a program called a device driver that acts as a translator, converting general commands from an application into specific commands that the device understands.

Dictionary Attack

The dictionary attack is used on applications with encryption stronger than 40-bit. PRTK uses this method to recover passwords

Disk

A round plate on which data can be encoded. There are two basic types of disks: magnetic disks and optical disks.

E

EnScript (also “e script”)

EnScript is a language and API that has been designed to operate within the EnCase environment. EnScript is compatible with the ANSI C++ standard for expression evaluation and operator meanings but contains only a small subset of C++ features. In other words, EnScript uses the same operators and general syntax as C++ but classes and functions are organized differently.

Evidence Item

A physical drive, a logical drive or partition, or drive space not included in any partitioned virtual drive.

F

File Allocation Table (FAT)

A table that the operating system uses to locate files on a disk. A file may be divided into many sections that are scattered around the disk. The FAT keeps track of all these pieces.

There is a field in the Boot Record that specifies the number of FAT copies. With FAT12 and FAT16, MS-DOS uses only the first copy, but the other copies are synchronized. FAT32 was enhanced to specify which FAT copy is the active one in a 4-bit value part of a Flags field.

Think of the FAT as a singly linked list. Each of the chains in the FAT specify which parts of the disk belong to a given file or directory.

A file allocation table is a simple array of 12-bit, 16-bit, or 32-bit data elements. Usually there will be two identical copies of the FAT.

FAT12: The oldest type of FAT uses a 12-bit binary number to hold the cluster number. A volume formatted using FAT12 can hold a maximum of 4,086 clusters, which is 2^{12} minus a few values (to allow for reserved values to be used in the FAT). FAT12 is most suitable for very small volumes, and is used on floppy disks and hard disk partitions smaller than about 16 MB (the latter being rare today.)

FAT16: The FAT used for older systems, and for small partitions on modern systems, uses a 16-bit binary number to hold cluster numbers. When you see someone refer to a FAT volume generically, they are usually referring to FAT16, because it is the de facto standard for hard disks, even with FAT32 now more popular than FAT16. A volume using FAT16 can hold a maximum of 65,526 clusters, which is 2^{16} less a few values (again for reserved values in the FAT). FAT16 is used for hard disk volumes ranging in size from 16 MB to 2,048 MB. VFAT is a variant of FAT16.

FAT32: The newest FAT type, FAT32 is supported by newer versions of Windows, including Windows 95's OEM SR2 release, as well as Windows 98, Windows ME, and Windows 2000. FAT32 uses a 28-bit binary cluster number—not 32 because 4 of the 32 bits are reserved. 28 bits is still enough to permit very large volumes—FAT32 can theoretically handle volumes with over 268 million clusters, and will theoretically support drives up to 2 TB in size. To do this, however, the size of the FAT grows very large.

VFAT features the following key improvements compared to FAT12 and FAT16:

- **Long File Name Support**: Prior to Windows 95, FAT was limited to the eleven-character (8.3) file name restriction. VFAT's most important accomplishment enabled the use of long file names by the Windows 95 operating system and applications written for it, while maintaining compatibility with older software that had been written before VFAT was implemented.

- **Improved Performance**: The disk access and file system management routines for VFAT were rewritten using 32-bit protected-mode code to improve performance. At the same time, 16-bit code was maintained, for use when required for compatibility.
- **Better Management Capabilities**: Special support was added for techniques like disk locking to allow utilities to access a disk in exclusive mode without fear of other programs using it in the meantime.

File Header

The data at the beginning of a file that identifies the file type: .gif, .doc, .txt, etc.

File Footer

The data at the end of the file signifying the file is complete and allows the file to be understood by the operating system.

File Item

Any item FTK can parse from the evidence. This includes complete files as well as sub-elements such as graphics, files, or OLE objects embedded in other files; deleted items recovered from unallocated space; and so forth.

File Slack

Unused space. Operating systems store files in fixed-length blocks called clusters. Because few files are a size that is an exact multiple of the cluster size, there is typically unused space between the end of the file and the end of the last cluster used by that file.

Forensic Image

A process where all areas of a physical disk are copied, sector by sector, to storage media. This image may be a raw file, as in the case of the Linux utility DD, or it may be a forensically correct copy, such as SPADA provides. These images replicate exactly all sectors on a given storage device. All files, unallocated data areas, and areas not normally accessible to a user are copied.

Forensically Prepared Media

Digital media (such as a diskette, tape, CD, hard drive) that is sanitized (wiped clean) of all data. This means computer media that may be sanitized up to the Department of Defense standards 5220.22-M (National Industrial Security Program Operating Manual Supplement) using software wipe utilities such as Dan Mares (Maresware) Declassify, New Technologies Inc (NTI) Disk Scrub or M-Sweep Pro or Symantec (Norton) WipeInfo to remove all data by overwriting the existing data with random or pre-defined characters. The Linux OS may also be used to write out a value of zero (0) to a device.

The media is then examined using tools to determine that no data exists (MD5, SHA-1 or Diskedit). The partition information is removed and the media is sanitized from the physical address of (cylinder/head/sector) 0/0/1 to the physical (versus logical) end of the media.

The partition information is removed and the media is sanitized from the physical address of (cylinder/head/sector) 0/0/1 to the physical (versus logical) end of the media. This process involves using a program such as I-wipe, Encase, Linux, Drivespy, SPADA or any program capable of writing multiple passes of a single character over the entire drive.

Checksum is a form of redundancy check, a very simple measure for protecting the integrity of data by detecting errors in data. It works by adding up the basic components of a message, typically the bytes, and storing the resulting value. Later, anyone can perform the same operation on the data, compare the result to the authentic checksum and (assuming that the sums match) conclude that the message was probably not corrupted.

Redundancy check is extra data added to a message for the purposes of error detection and error correction.

The value of the checksum of forensically prepared media will be zero (0) provided the write process is done using zeros.

G

Graphic Image Files

Computer graphic image files such as photos, drawings, etc. Come in various standard formats. Some of the most common file types include but are not limited to Joint Photographic Experts Group (JPEG, JPG), Bitmap (BMP), Graphics Interchange Format (GIF, JFIF) and AOL image file (ART).

Golden Dictionary

The Golden Dictionary file, ADPasswords.dat, contains all recovered passwords for all PRTK sessions on the current computer. It is stored in the AccessData program directory (C:\Program Files\AccessData\Recovery\). Recovered passwords are used as the first level of attack in all password recovery sessions. Most people use the same password for different files, so recovering the password for a simple file often opens the door to more difficult files.

Graphic Interchange Format (GIF)

A common graphics format that can be displayed on almost all Web browsers. GIFs typically display in 256 colors and have built-in compression. Static or animated GIF images are the most common form of banner creation.

H

Hard Disk (Drive)

A magnetic disk on which you can store computer data. The term hard is used to distinguish it from a soft or floppy disk. Hard disks hold more data and are faster than floppy disks. A hard disk, for example, can store anywhere from 10 megabytes to several gigabytes, whereas most floppies have a maximum storage capacity of 1.4 megabytes.

Hashing

Generating a unique alphanumeric value based on a file's contents. The alphanumeric value can be used to prove that a file copy has not been altered in any way from the original. It is statistically impossible for an altered file to generate the same hash number.

Head

The mechanism that reads data from or writes data to a magnetic disk or tape. Hard disk drives have many heads, usually two for each platter.

Hexadecimal

The base-16 number system, which consists of 16 unique symbols: the numbers zero through nine and the letters A to F. For example, the decimal number 15 is represented as F in the hexadecimal numbering system. The hexadecimal system is useful because it can represent every byte (eight bits) as two consecutive hexadecimal digits. It is easier for humans to read hexadecimal numbers than binary numbers.

L

Legal Matter

Legal Matters are titles given to collections of electronic data to be used as evidence in a court of law against someone suspected of illegal activity. Legal Matters can be actual lawsuits or suspect activity.

Logical Disk

M

Markov Permutation

The Markov permutation records the times certain words, letters, punctuation, and spaces occur together in a given amount of text, then generates random output that has the same distribution of groups.

For example: if you were to scan through the text and create a huge frequency table of what words come after the words "up the," you might find "tree," "ladder," and "creek" most often. You would then generate output from the words "up the," and get the results "up the tree," "up the creek," and "up the ladder" randomly.

If the words “up the” were followed most frequently by the word “creek” in your sample text, the phrase “up the creek” would occur most frequently in your random output.

Andrey Andreyevich Markov (June 14, 1856–July 20, 1922) was a Russian mathematician.

Memory

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips; the word storage is used for memory that exists on tapes or disks. Moreover, the term memory is usually used as shorthand for physical memory, which refers to the actual chips capable of holding data.

Message Digest 5

A 128-bit digital fingerprint based on a file's content. An algorithm created in 1991 by Professor Ronald Rivest of RSA that is used to create digital signatures, or a 128-bit digital fingerprint based on a file's content. Message Digest 5 (MD5) takes as input an arbitrary-length file and outputs a fixed-length number referred to as a hash or digest. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest. When using a one-way hash function, one can compare a calculated message digest against the message digest that is decrypted with a public key to verify that the message hasn’t been changed. This comparison is called a hash check. The number is derived from the input in such a way that it is computationally infeasible to derive any information about the input from the hash. It is also computationally infeasible to find another file that will produce the same output.

MD5 hashes are used by the KFF to identify known files.

Metadata

Literally data about data. Metadata describes how, when, and by whom a particular set of data was collected and how the data is formatted. Metadata is essential for understanding information stored in data warehouses and has become increasingly important in XML-based Web applications.

Mount

To make a mass storage device available to the OS, or to a user or user group. In may also mean to make a device physically accessible. In a Unix environment, the mount command attaches discs or directories logically rather than physically. The Unix mount command makes a directory accessible by attaching a root directory of one file system to another directory, which makes all the file systems usable as if they were subdirectories of the file system they are attached to. Unix recognizes devices by their location, while Windows recognizes them by their names (C: drive, for example). Unix organizes directories in a tree-like structure in which directories are attached by mounting them on the branches of the tree. The file system location where the device is attached is called a mount point. Mounts may be local or remote. A local mount connects disk drives on one machine so that they behave as one logical system. A remote mount uses Network File System (NFS) to connect to directories on other machines so that they can be used as if they were all part of the user's file system.

N

NT File System (NTFS)

One of the file systems for the Windows NT operating system (Windows NT also supports the FAT file system). NTFS has features to improve reliability, such as transaction logs to help recover from disk failures. To control access to files, you can set permissions for directories or individual files. NTFS files are not accessible from other operating systems, such as DOS. For large applications, NTFS supports spanning volumes, which means files and directories can be spread out across several physical disks.

P

Pagefile (.sys)

The paging file is the area on the hard disk that Windows uses as if it were random access memory (RAM). This is sometimes known as virtual memory. By default, Windows stores this file on the same partition as the Windows system files.

Pretty Good Privacy

A common symmetric encryption system used for exchanging files and email. It provides both privacy and authentication.

Public Data Repositories

R

RC4

RC4, or ARC4, is a variable key-length stream cipher designed by RSA. Stream ciphers are key-dependent, pseudo-random number generators whose output is XORed with the data <plaintext> XOR <random-looking stream> = <random-looking ciphertext>. Because XOR is symmetric (in other words, [A XOR B] XOR B = A), XORing the ciphertext with the stream again returns the plaintext. Microsoft Word and Excel use RC4 and a 40-bit key to encrypt their files. An exhaustive key space attack has a much better chance at succeeding with a 40-bit key space.

S

Sector

A sector is a group of bytes within a track and is the smallest group of bytes that can be addressed on a drive. There are normally tens or hundreds of sectors within each track. The number of bytes in a sector can vary, but is almost always 512. The maximum number of sectors in a cluster is 64. CDROMS normally have 2048 bytes per sector. Sectors are numbered sequentially within a track, starting at 1. The numbering restarts on every track, so that "track 0, sector 1" and "track 5, sector 1" refer to different sectors. Modern drives use a system known as Logical Block Addressing (LBA) instead of CHS to track sectors.

During a low-level format, hard disks are divided into tracks and sectors. The tracks are concentric circles around the disk and the sectors are segments within each circle. For example, a formatted disk might have 40 tracks, with each track divided into ten sectors.

Physical sectors are relative to the entire drive. Logical sectors are relative to the partition.

Secure Hash Algorithm

A 160-bit digital fingerprint based on a file's content. Designed by the National Institute of Standards and Technology (NIST), Secure Hash Algorithm (SHA) takes as input an arbitrary-length file and outputs a fixed-length number referred to as a hash or digest. The number is derived from the input in such a way that it is computationally impossible to derive any information about the input from the hash. It is also computationally impossible to find another file that will produce the same output. SHA-1 hashes are used by the KFF to identify known files.

FTK uses SHA-1 and SHA-256. The KFF library contains some A hashes.

SHA

The SHA (Secure Hash Algorithm) family is a set of related cryptographic hash functions. The most commonly used function in the family, SHA-1, is employed in a large variety of popular security applications and protocols, including TLS, SSL, PGP, SSH, S/MIME, and IPSec. SHA-1 is considered to be the successor to MD5, an earlier, widely-used hash function. The SHA algorithms were designed by the National Security Agency (NSA) and published as a US government standard.

The first member of the family, published in 1993, is officially called SHA; however, it is often called SHA-0 to avoid confusion with its successors. Two years later, SHA-1, the first successor to SHA, was published. Four more variants have since been issued with increased output ranges and a slightly different design: SHA-224, SHA-256, SHA-384, and SHA-512—sometimes collectively referred to as SHA-2.

Attacks have been found for both SHA-0 and SHA-1. No attacks have yet been reported on the SHA-2 variants, but since they are similar to SHA-1, researchers are worried, and are developing candidates for a new, better hashing standard.

Spool (spooling, print spool)

Acronym for Simultaneous Peripheral Operations On-Line, spooling refers to putting jobs in a buffer, a special area in memory or on a disk where a device can access them when it is ready. Spooling is useful because devices access data at different rates. The buffer provides a waiting station where data can rest while the slower device catches up.

The most common spooling application is print spooling. In print spooling, documents are loaded into a buffer (usually an area on a disk), and then the printer pulls them off the buffer at its own rate. Because the documents are in a buffer where they can be accessed by the printer, you can perform other operations on the computer while printing takes place in the background. Spooling also lets you place a number of print jobs on a queue instead of waiting for each one to finish before specifying the next one.

Slack Space (File and RAM)

Files are created in varying lengths depending on their contents. DOS, Windows and Windows NT-based computers store files in fixed length blocks of data called clusters. Rarely do file sizes exactly match the size of one or multiple clusters perfectly. The data storage space that exists from the end of the file to the end of the last cluster assigned to the file is called file slack. Cluster sizes vary in length depending on the operating system involved and, in the case of Windows 95, the size of the logical partition involved. Larger cluster sizes mean more file slack and also the waste of storage space when Windows 95 systems are involved.

File slack potentially contains randomly selected bytes of data from computer memory. This happens because DOS/Windows normally writes in 512 byte blocks called sectors. Clusters are made up of blocks of sectors. If there is not enough data in the file to fill the last sector in a file, DOS/Windows makes up the difference by padding the remaining space with data from the memory buffers of the operating system. This randomly selected data from memory is called RAM Slack because it comes from the memory of the computer.

RAM Slack can contain any information that may have been created, viewed, modified, downloaded or copied during work sessions that have occurred since the computer was last booted. Thus, if the computer has not been shut down for several days, the data stored in file slack can come from work sessions that occurred in the past.

RAM slack pertains only to the last sector of a file. If additional sectors are needed to round out the block size for the last cluster assigned to the file, then a different type of slack is created. It is called drive slack and it is stored in the remaining sectors which might be needed by the operating system to derive the size needed to create the last cluster assigned to the file. Unlike RAM slack, which comes from memory, drive slack is padded with what was stored on the storage device before. Such data could contain remnants of previously deleted files or data from the format pattern associated with disk storage space that has yet to be used by the computer.

For example, take a file that is created by writing the word "Hello." Assuming that this is the only data written in the file and assuming a two sector cluster size for the file, the data stored to disk and written in file slack could be represented as follows:

Hello+++++++|————(EOC)

RAM Slack is indicated by "+"

Drive Slack is indicated by "–"

File Slack is created at the time a file is saved to disk. When a file is deleted under DOS, Windows, Windows 95, Windows 98 and Windows NT/2000/XP, the data associated with RAM slack and drive slack remains in the cluster that was previously assigned to the end of the deleted file. The clusters which made up the deleted file are released by the operating system and they remain on the disk in the form of unallocated storage space until the space is overwritten with data from a new file.

File slack potentially contains data dumped randomly from the computer's memory. It is possible to identify network login names, passwords, and other sensitive information associated with computer usage. File slack can also be analyzed to identify prior uses of the subject computer and such legacy data can help the computer forensics investigator. File slack is not a trivial item. On large hard disk drives, file slack can involve several hundred megabytes of data. Fragments of prior email messages and word processing documents can be found in file slack. From a computer forensic standpoint, file slack is very important as both a source of digital evidence and security risks

String Searches

A string search is a data string containing standard text or non-text data. The term may be a word, phrase or an expression. Keyword searches are designed to aid in the identification of potentially relevant data on the examined media.

Superuser Administrator

A person with unlimited access privileges who can perform any and all operations on the computer and within the operating system and file system. These privileges do not necessarily transfer to the applications installed on the computer.

Symmetric Encryption

A type of encryption in which the encryption and decryption keys are the same. Some common symmetric encryption systems are Data Encryption Standard, Triple-DES, Pretty Good Privacy, BestCrypt, and Advanced Encryption Standard.

T

Task

Tasks provide investigators and reviewers with a means of tracking the progress of case review. Administrators assign Reviewers specific tasks in the case and a specific group of data. The assigned task allows the reviewer to know which filters to apply to the data set for review.

Thumbnail

A smaller-sized version of a graphics image.

U

Unallocated Space

Also called **Unused Disk Area** or free space, it consists of all the clusters on a drive that are not currently assigned to a file. Some of these clusters may still contain data from files that have been deleted but not yet overwritten by other files.

Until the first file is written to the data storage area of a computer storage device, the clusters are unallocated by the operating system in the File Allocation Table (FAT). These unallocated clusters are padded with format pattern characters and the unallocated clusters are not of interest to the computer forensics specialist until data is written to the clusters. As the computer user creates files, clusters are allocated in the File Allocation Table (FAT) to store the data. When the file is deleted by the computer user, the clusters allocated to the file are released by the operating system so new files and data can be stored in the clusters when needed. However, the data associated with the deleted file remains behind. This data storage area is referred to as unallocated storage space and it is fragile from an evidence preservation standpoint. However, until the unallocated storage space is reassigned by the operating system, the data remains behind for easy discovery and extraction by the computer forensics specialist. Unallocated file space

potentially contains intact files, remnants of files and subdirectories and temporary files, which were transparently created and deleted by computer applications and also the operating system. All of such files and data fragments can be sources of digital evidence and also security leakage of sensitive data and information.

URL

Abbreviation of Uniform Resource Locator, the global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use and the second part specifies the IP address or the domain name where the resource is located.

User

Those who use AccessData computer forensic programs to collect, review, and process data for legal cases are called Users. An Administrator or user with administrative rights can create users and designate their roles and user rights.

V

Volume

A volume refers to a mounted partition. There may be only one volume on a disk, such as a floppy disk or a zip disk. There may be several volumes on a disk as on a partitioned hard drive. A volume is a logical structure, not a physical device. There can be up to 24 of these logical volumes on a disk and they show up as drive "c," "d," or "e" in DOS.

Volume Boot Sector

Since every partition may contain a different file system, each partition contains a volume boot sector which is used to describe the type of file system on the partition and usually contains boot code necessary to mount the file system